

Teknologi og lov

Arbeidsgiver og arbeidstakers rettigheter og plikter ved bruk av e-post i forhold til den "nye" e-postforskriften

Kandidatnummer: 398

Leveringsfrist: 25.4.2007, klokken 12:00

Til sammen ca 17 500 ord

Innholdsfortegnelse

1. INNLEDNING	4
2. SAMFUNNSSITUASJONEN	5
3. FORHISTORIE TIL DEN NYE "E-POSTLOVEN"	8
4. BEGREPSAVKLARING OG SENTRALE BEGREPER	10
4.1 Definisjon av e-post	11
4.2 Definisjon av elektronisk utstyr, kommunikasjon og lagrede opplysninger	13
4.3 Definisjon av overvåking	14
4.4 Definisjon av arbeidstaker, arbeidsgiver	15
4.5 Definisjon av elever og studenter, frivillige og tillitsvalgte med mer	17
5. KJERNEPUNKTER I FORSKRIFTSFORSLAGET	18
6. NORDISK RETT	18
7. GJELDENDE RETT VEDRØRENDE PERSONOPPLYSNINGER	20
7.1 Datatilsynets retningslinjer	22
7.2 Gjeldende rett vedrørende e-post spesielt	24
8. FORSKRIFTSFORSLAGET NEDSLAGOMRÅDET	27
8.1 Menneskerettigheter og EØS-rett	27
8.2 Personvern på arbeidsplassen i forhold til arbeidsmiljøloven	30
8.3 Postloven og arkivloven	34
8.4 Strafferett	35
8.5 Offentlighetsloven og tilsvarende lover	37
9. RETTSLIG BETRAKTNINGER	38
9.1 Rettslige betraktninger vedrørende e-post generelt	38
9.2 Jurisdiksjon	42
8.3 Virksomhetsrelatert e-post blir "privat" e-post	43
8.4 Mellomlagring av e-post i forbindelse med informasjonssikkerhet	43
8.5 Interne rutiner og instruksjer	45
9.6 Virksomhetens og 3. parts juridiske interesser	48
9.7 Eierskap til datasystemet og lukkede datanett	51
9.8 Elever og studenter	53
9.9 Arbeidsforholdet opphører	54

9.10 Samtykke	54
10. SAMMENDRAG.....	56
11. LITTERATURLISTE.....	58

1. Innledning

E-posthåndtering reiser mange spørsmål, både av juridisk og pratisk art. Rettstilstanden på dette området har vært noe uklar, og med bakgrunn i dette har Forsynings- og administrasjonsdepartementet sendt ut på høring forslag om ny ”e-postlov”¹ – *”Forslag til regler om arbeidsgivers tilgang til ansattes e-post mv – endring av personopplysningsloven § 3 og § 46, nytt kapittel i personlysningsforskriften og ny bestemmelse i arbeidsmiljøloven”* (heretter kalt høring).

Det er Fornyings- og administrasjonsdepartementet som har sendt ut høringen. Denne ble sendt ut i oktober 2006, med høringsfrist 17. januar 2007.

Denne oppgaven vil ta for seg innholdet i høringen i forhold til hva og hvilke forhold den forsøker å regulere i forhold til e-post. Ettersom det finnes lite rettspraksis, og da særlig sett i forhold til den teknologiske utviklingen av kommunikasjonssystemer, vil oppgaven i viss grad basere seg på de lega ferenda betraktninger. Oppgaven er på bakgrunn av dette også skrevet i et retts sosiologisk perspektiv.

Videre vil oppgaven legge vekt på de prinsipale betraktninger i e-posthøringen. I korthet betyr dette at man ikke kommer til å gjennomgå fortolkninger av rettskildetekster spesielt i dybden, spesielt der det ikke er nødvendig for å få frem de prinsipale betraktninger.

Oppgaven vil heller ikke ta opp spørsmålet rundt innsyn, beslag, overvåkning etc av e-post og tekniske innretninger i forhold til myndighetene, og særhjemmelene som finnes i forbindelse med dette. Det en her særlig tenker på er politi- og påtalemyndigheten, myndighetenes overvåking og etterretningsorganisasjoner. Oppgaven vil også avgrenses til i hovedsak å gjelde e-postproblematikk, og tar ikke opp de andre problemstillinger som angår lagring, arkivering og andre tekniske innretninger som høringen også tar sikte på å regulere.

Med bakgrunn i høringsuttalelsene antas det at slik forskriftsforslaget er lagt frem, at den reiser flere problemstillinger enn den løser. Oppgaven tar derfor ikke for seg en konkret problemstilling, men gir heller en kort oversikt over mulige problemstillinger som vil kunne komme frem hvis forskriftsforslaget vedtas i den form som den foreligger i dag.

¹ Se side 1 i høringsnotatet.

Det blir videre henvist til en del internettsider i forbindelse med kildehenvisning. Med bakgrunn i Internettets natur, kan det hende at når man slår opp internettdressen i ettertid at websiden ikke finnes, er flyttet eller at serveren som siden lå på er nede. På det tidspunktet som oppgaven ble skrevet fantes imidlertid disse internettsidene.

Oppbygningen av oppgaven er slik at først gjennomgås samfunnssituasjonen, deretter forhistorie til den ”nye” e-postforskriften, begrepsavklaringer og kjernepunkter i forskriftsforslaget. Så vil man gjennomgå nordisk og gjeldende norsk rett. Deretter vil man se på hjemmelsgrunnlaget for forskriftsforslaget, og forsette med å ta opp konkrete problemstillinger som er forbundet med selve reglene i forskriftsforslaget. Til slutt kommer en oppsummering med avsluttende kommentarer.

2. Samfunnssituasjonen

I dagens samfunn er grensene mellom arbeid og fritid blitt betydelig vevd inn i hverandre. Dette skyldes flere ting, men det pekes særs på at teknologien har blitt billigere, mobilitet og globalisering.

At teknologien har blitt billig innebærer at ”menigmann” har råd til kjøpe relativt avansert utstyr for en rimelig penge. Nå koster for eksempel en ”hypermoderne” PDA² integrert med mobiltelefon, videokamera, GPS³ og med ”full” datamaskinkapasitet, noen få tusen kroner. Dette i motsetning til for noen få år tilbake, hvor en ”simpel” datamaskin kostet opptil femti tusen kroner – noen som de færreste hadde råd til.

² PDA, Personal digital assistants

³ GPS, Global Positioning System

Med bakgrunn i dette har også de fleste husstander i Norge en egen datamaskin⁴.

Med bakgrunn i mobilitet og globalisering har grensene mellom arbeid og fritid også blitt betydelig visket ut. Moderne kommunikasjonsløsninger gjør at man er langt mer tilgjengelig enn tidligere. Med bakgrunn i dette har arbeidsgiver de siste årene beveget seg inn i arbeidstakerens private sfære gjennom resultatbaserte løsninger (dvs at man kan jobbe hvor og når man vil, så lenge man oppnår det målsatte resultatet), mobiltelefoni, hjemmekontor, bærbare løsninger osv. For eksempel har mange bedrifter i dag mobiltelefoni som den eneste telefoniløsning.

Globaliseringen har ført til at man pga tidsforskjeller må være tilgjengelig, for eksempel i en chat eller telefonkonferanse, på andre tider enn en "normal" norsk arbeidsdag. I tillegg er det blitt mer vanlig at man arbeider i multinasjonale selskap, hvor ansatt i Norge ofte i tillegg må forholde seg til det internasjonale selskapets policy og regler.

Selv om arbeidsgiver ofte stiller "standard" utstyring, som for eksempel mobiltelefon, datamaskin eller PDA, er det ikke uvanlig at arbeidstakeren selv invester i "high-tech" utstyr og heller benytter dette både privat og i arbeid. Denne konstellasjonen kan ofte også komme arbeidsgiver til gode. For eksempel at en arbeidsgiver utstyret en selger med en vanlig mobiltelefon. Selger kjøper heller en privat PDA med GPS og telefon (men hvor telefonabonnementet kanskje er betalt av arbeidsgiver), slik at han ikke bruker så lang tid til å finne frem, og kan dermed kanskje besøke flere kunder på en dag.

Med bakgrunn i dette antas det at arbeidsgiver må forvente at arbeidstakeren tar med seg mer av den private sfæren inn i arbeidssituasjonen. Og i flere jobber kan det være vanskelig å trekke skille mellom privat og arbeidsrelatert bruk av maskinressurser, e-post og Internett.

Undersøkelse utført av Kelly Services⁵ viser at 51 % av norske arbeidstakere mener at det å bruke arbeidsgivers internetttilkobling til private formål i arbeidstiden ikke er noe problem.

⁴ TNS Gallup vedrørende internettbruk, se <http://www.tns-gallup.no> under linken "Medier". Internettvaner første kvartal 2007; Befolkningen 12 år + har 85 % av den norske befolkning, dvs ca 3 334 000 personer, tilgang til Internett. 80 % dvs ca 3 138 000 personer bruker Internett månedlig og 65 % dvs ca 2 549 000 personer bruker Internett daglig. Daglige Internett brukere skiller seg fra resten av befolkningen. Det er flere menn enn kvinner, flere unge enn eldre, flere med høy utdanning og høy inntekt som bruker nettet daglig kontra i befolkningen 12 år + generelt.

Rapporter fra Transportøkonomisk institutt, TØI rapport 789/2005 og TØI rapport 800/2005⁶, viste at 28 % av de spurte mente det var problematisk om arbeidsgiver kunne se hvem man utvekslet e-post med. 58 % at det var problematisk om arbeidsgiver leste innholdet i e-posten. 84 % har stor eller noe tillit til behandling av personopplysninger hos arbeidsgivere generelt, mens 79 % er svært lite eller lite bekymret for misbruk av personopplysninger der arbeidsgiver har personopplysninger. 65 % av de spurte representantene for virksomhetene var uenig om at arbeidsgiveren bør ha ubegrenset rett til å lese all e-post som de ansatte sender og mottar på jobben. 58 % av arbeidstakerene mente at det er svært eller noe problematisk at arbeidsgiver eller lærersted skal kunne se innholdet i e-post. Undersøkelsene skiller ikke mellom innsyn i virksomhetsrelatert og privat e-post⁷.

Dette gir et sammensatt og komplisert bilde med to interesser som vil kunne stå mot hverandre. På den ene siden ansattes personverninteresser, og på den andre siden arbeidsgivers ønske om å iverksette kontrolltiltak og sikre en forsvarlig og effektiv drift. En virksomhet kan ha interesse i å gjøre seg kjent med arbeidstakernes ”digitale bevegelser”, det kan også tenkes at virksomheten er forpliktet til å gjøre dette, eller sikre at arkivverdig materiale ikke går tapt.

Man vil derfor stå ovenfor en interesseavveining mellom arbeidsgivers legitime interesser, rettigheter og plikter for å drive virksomheten effektivt og lovlig, mot ansattes rett til beskyttelse av privatlivets fred på arbeidsplassen.

Denne avveiningen har vist seg vanskelig å gjennomføre i praksis. Datatilsynet har behandlet flere saker hvor arbeidsgiver har foretatt innsyn i ansattes e-post, og hvor dette har vært fremstilt som brudd på gjeldende regler på området.

⁵ Se <http://www.idg.no/karriere/karrierenyheter/article2849.ece>

⁶ ”Setter vår lit til Storebror ... og alle småbrødre med? Befolkningens holdning til og kunnskap om personvern, TØI rapport 789/2005. *Behandling av personopplysninger i norske virksomheter*, En spørreundersøkelse om personvern og personopplysningsloven, TØI rapport 800/2005.

⁷ Tallene fremkommer også i høringsnotatet.

Datatilsynets anmeldte også to selskaper for brudd på personopplysningsloven høsten 2005, og ett selskap i 2006. Datatilsynet har også mottatt flere henvendelser fra arbeidsgivere og arbeidstakere, med spørsmål om hvor grensen for lovlig innsyn går⁸.

For å avklare rettstilstanden på dette feltet er det fremmet forslag om å endre lov om behandling av personopplysninger 14. april 2000 nr 31 (personopplysningsloven), slik at den gir hjemmel til å fastsette særskilte regler om arbeidsgivers innsyn i arbeidstakers e-post og annen bruk av elektroniske virkemidler på arbeidsplassen.

3. Forhistorie til den nye "e-postloven"

Datatilsynet⁹ ble opprettet 1. januar 1980 og er et uavhengig forvaltningsorgan, underlagt Fornyings- og administrasjonsdepartementet. Datatilsynet har sine oppgaver lovhjemlet i personopplysningsloven § 42. Med bakgrunn i dette har Datatilsynet gitt retningslinjer¹⁰ i forbindelse med innsyn og overvåking av e-post og andre tekniske innretninger.

Selv om Datatilsynet har gitt retningslinjer, har rettstilstanden på dette området vært noe uklar. Dette med særlig grunn i at Høyesterett ikke direkte har behandlet spørsmålet om innsynsrett og forskjellige former overvåkning av e-post og bruk av IT-verktøy.

Bl.a. med bakgrunn i dette la Arbeidslivslovutvalget i NOU 2004: 5¹¹ om ny arbeidsmiljølov, fram et forslag til en bestemmelse om arbeidsgivers rett til innsyn i arbeidstakernes e-post.

Utvalget foreslo et nytt kapittel om kontroll og overvåking. Hovedregelen var at arbeidsgiver bare skal kunne iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold, og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren. I tillegg ble det foreslått en særregel om kontroll av e-post og andre private elektroniske opplysninger.

Forslaget hadde følgende ordlyd:

⁸ Se <http://www.datatilsynet.no> vedrørende arbeidslivet og side 1 i høringsnotatet.

⁹ Se Datatilsynets hjemmesider, http://www.datatilsynet.no/templates/AboutPage____220.aspx

¹⁰ Datatilsynet retningslinjer i forbindelse med e-post http://www.datatilsynet.no/templates/article____201.aspx

¹¹ Et arbeidsliv for trygghet, inkludering og vekst

(1) Arbeidsgiver har ikke rett til innsyn i arbeidstakers private e-post eller andre private elektroniske opplysninger, med mindre arbeidstaker har gitt skriftlig samtykke til innsyn.

(2) Første ledd gjelder ikke dersom det foreligger fare for sikkerheten eller informasjonssikkerheten i virksomheten, dersom det er saklig grunn til å mistenke arbeidstaker for å ha benyttet arbeidsgivers elektroniske utstyr på en måte som kan gi grunnlag for oppsigelse eller avskjed eller dersom det foreligger en annen særlig grunn som gjør at innsyn er nødvendig.

I forslaget slås det fast at innsyn i arbeidstakernes private e-post uten samtykke er forbudt. Utvalget brukte ikke begrepet virksomhetsrelatert e-post i reguleringsforslaget, men synes å legge til grunn at arbeidsgiver har adgang til å lese slik post.

Utvalget pekte på at arbeidsgiver kunne komme i skade for å åpne privat e-post ved kontroll av virksomhetsrelatert e-post. Dersom arbeidsgiver har handlet i god tro, vil innsynet i privat e-post i en del tilfeller kunne skyldes at arbeidstakeren ikke har sørget for å markere skillet mellom virksomhetsrelatert og privat korrespondanse på en god nok måte, mens det i andre tilfeller kunne være tale om brudd på interne regler.

Datatilsynet påpekte at det var behov for en klarere regulering, og mente at det var behov for langt mer detaljerte bestemmelser enn det som var foreslått. I tillegg mente Datatilsynet at forslaget materielt sett ikke var tilstrekkelig ut fra et personvernspunkt. På bakgrunn av Datatilsynets innvendinger mot forslaget, og at det allerede pågikk et arbeid med å utarbeide forskrifter om dette, fremmet ikke Arbeids- og sosialdepartementet forslag til regler om innsyn i e-post på det daværende tidspunkt, jf. Ot. prp. nr. 49 (2004-2005)¹².

Med bakgrunn i dette har Fornyings- og administrasjonsdepartementet sendt ut på høring et forskriftsforslag (heretter kalt forskriftsforslag) som skal regulere innsyn i e-post, elektronisk utstyr, og annen elektronisk kommunikasjon og av elektronisk lagrede opplysninger. Forskriftsforslaget er utarbeidet av deltakere fra Justisdepartementet, Datatilsynet og Fornyings- og administrasjonsdepartementet.

¹² Se punkt 12.6.5 vedrørende "Kontroll av privat e-post".

Høringen¹³ ble sendt ut i oktober 2006 med høringsfrist 17. januar 2007. Det har innkommet flere høringsuttalelser innen fristen, men også etter at fristen ble forlenget for enkelte høringsinstanser.

Støtte til forskriftsforslaget varierer avhengig av ståstedet til høringsinstansene. Det virker som om støtten er sterkere fra høringsinstansene hvor personverninteressene står sterkt, og motsatt hvor ivaretagelsen av de kommersielle interessene er fremtredende.

Ut fra høringsuttalelsene møter forskriftsforslaget sterk kritikk på en rekke punkter. Dette gjelder bl.a. sammensetning av gruppen som står bak forslaget, at forskriftsforslaget ikke er teknologinøytral eller tar hensyn til forskjellige former for teknologi, praktiske teknologiske problemstillinger knyttet til e-post, samt juridiske betenkninger vedrørende plassering og det materielle innholdet i forskriftsforslaget. Det anmerkes også at forskriftsforslaget også får full støtte av enkelte høringsinstanser uten bemerkninger.

4. Begrepsavklaring og sentrale begreper

Forskriftsforslaget vil være hjemlet i den endrede personopplysningsloven § 3, som vil lyde (*endringen i kursiv*):

§ 3 fjerde ledd første punktum

"Kongen kan gi forskrift *om særskilte former for behandling av personopplysninger*, og om behandling av personopplysninger i særskilte virksomheter eller bransjer."

Forskriftsforslaget § 9-1, Virkeområdet, inneholder hva som søkes regulert og inneholder en rekke sentrale begreper. De begrepene som er av særlig interesse, er arbeidstaker, arbeidsgiver, elever og studenter, frivillige og tillitsvalgte i foreninger og organisasjoner, e-post, overvåking, elektronisk utstyr, elektronisk kommunikasjon og elektronisk lagrede opplysninger.

Nedenfor gjennomgås disse begrepene.

¹³ se <http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2006/Forslag-til-regler-om-arbeidsgivers-adgang-til-ansattes-e-post-mv.html?id=270942>

4.1 Definisjon av e-post

Forskriftsforslaget har selv ingen definisjon, og henviser heller ikke til andre lover i forhold til definisjonen av begrepet e-post. Det antas at man med begrepet e-post i forskriftsforslaget henviser til dagens alminnelige oppfatning av hva e-post er.

I følge Kunnskapsforlagets¹⁴ blå språk- og ordbokstjeneste er e-post definert som elektronisk post; e-mail.

Den ”alminnelige” oppfatning¹⁵ av e-post antas å være at en e-post ”er en melding som sendes fra eller til en person via et datanettverk og som kan inneholde tekst, data, eller tale”. Med data forstås her både programmer, filer, bilder, video med mer.

Ettersom forskriftsforslaget selv ikke definerer begrepet e-post, antas det at man sikter til dagens alminnelige oppfatning av ordet e-post og dertil innhold.

Markedsføringsloven § 2b, 4. ledd, har imidlertid definisjonen på e-post:

Med elektronisk post menes i denne bestemmelse enhver henvendelse i form av tekst, tale, lyd eller bilde som sendes via et elektronisk kommunikasjonsnett, og som kan lagres i nettet eller i mottakerens terminalutstyr inntil mottakeren henter den. Herunder omfattes tekst- og multimediemeldinger til mobiltelefon (SMS og MMS).

Definisjonen er hentet fra Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon), artikkel 2 bokstav h.

Selv om markedsføringsloven regulerer et annet forhold, gir definisjonen av e-post i markedsføringsloven et utgangspunkt på hva som ligger i begrepet fra lovgivers side.

¹⁴ Se <http://www.ordnett.no>

¹⁵ For å undersøke hvordan e-post begrepet oppfattes ble 426 personer spurt om hva de legger i begrepet e-post. Det er på bakgrunn av svarene den ”alminnelige” oppfatningen fremlegges. Undersøkelsen ble foretatt 6. januar 2007 – Sandvika storsenter, 109 personer, 9. januar 2007 – Oslo sentrum, 146 personer, 15. januar 2007 – Tromsø, 29 personer, og 8. februar 2007 Oslo, 142 personer. Spørsmålet som ble stilt var ”Hva forstår du med ordet e-post?”. Det var tilfeldig forbigående som ble spurt, og på forskjellige tidspunkter innen samme dag. Undersøkelsen er kun gjennomført for å få en pekepinn på folks oppfatning, og kan ikke tas som inntekt for noen vitenskapelig fortolkning eller metodikk som ligger bak undersøkelsen.

Markedsføringsloven § 2b bruker ordene ”tekst, tale, lyd eller bilde” og ikke ordet data. Programmer er antatt å gå innunder ordet data i forhold til den vanlige tekniske forståelsen. Spørsmålet blir da om passive programmer som er sendt via e-post vil kunne falle utenfor definisjonen, mens aktive programmer falle innenfor. Dette med bakgrunn i at når man kjører aktive programmer vil en aktiv handling i form av lyd, bilde eller tekst fremkomme på skjermen. Passive programmer viser ingen ting og kan sammenlikes med spionprogramvare. Disse kan for eksempel sende ut informasjon om brukerens internettvaner og kan senere benyttes til for eksempel lovlig markedsføring. Det ligger imidlertid utenfor denne oppgaven om slike programmer kan rammes av annen lovgivning, for eksempel straffeloven.

Videre er ordet tekst brukt. Spørsmålet er om tekst er definert det som er lese- og forståelsesbart for et menneske, eller om det er tekst generelt. Er for eksempel ren maskinkode (binærkode) innbefattet eller ikke i begrepet tekst? Ser man formålet med loven, må det antagelig kunne svares ja på dette spørsmålet. Dette særlig med bakgrunn i at forarbeidene til markedsføringsloven § 2 b bruker ordet ”vanlig” når man refererer til definisjonen (uten å definere ordet ”vanlig”), og at det for brukeren er tekst uavhengig om det er i 0 og 1 eller ord.

Innholdet i begge definisjonene (markedsføringslovens og den alminnelige oppfatning) viser at det må være en fysisk person som behandler mottak av e-posten. Videre at den må sendes via et elektronisk kommunikasjonsnett, og at man ser meldingen under ett (vedlegg blir da en del av meldingen) som inneholder tekst, tale, lyd, data eller bilde. I forhold til avsender kan denne være enten en fysisk person eller en automatisk maskingenerert melding.

Med bakgrunn i at rettskildedefaktorene trekker i samme retning, vil det i den videre fremstillingen ovennevnte forståelse legges til grunn (at mottaker må være et menneske) når man bruker begrepet e-post. Med denne definisjonen betyr det at automatiserte meldinger mellom datamaskiner eller tekniske innretninger, uavhengig om de inneholder personopplysninger eller ikke, og selv om de bruker tradisjonelt teknisk e-postsystem seg i mellom, vil falle utenfor definisjonen. Denne problemstillingen vil da heller ikke drøftes, men det anføres at problemstillingen i seg adresserer en rekke problemstillinger i forhold til personopplysningsloven, og som har vært lite behandlet i rettspleien.

Ser man hen til hvordan e-post er bygget opp, vil den bestå av tre komponenter. Det er selve meldingen, e-postadressen (for eksempel per.person@virksomhet.no) og e-postkassen (@virksomhet.no som kan sammenliknes med ordinær postkasse). Disse komponentene vil bli behandlet under punkt 7, ”Gjeldende rett”.

Ser man hen til selve den tekniske løsningen som e-post baserer seg på, inneholder den en serverklient-basert løsning. Dvs at når A vil sende en melding til B, vil A sende meldingen fra sin e-postklient til sin e-postserver. Her vil meldingen mellomlagres før den sendes videre til B sin e-postserver. B kan da logge seg på sin e-postserver (dette skjer som regel automatisk i forhold til oppsettet i B sin e-postklient) og hente meldingen fra sin e-postserver til sin e-postklient og lese denne. B kan også velge å lese meldingen direkte på sin e-postserver (meldingen vil da bli liggende på e-postserveren hos B) uten å hente denne ned til sin e-postklient¹⁶.

Mellom e-postserverne og mellom e-postserveren og e-postklienten, vil det kunne ligge flere typer av automatisert programvare, for eksempel spamfilter, programmer for innholdsjekk, mottiltak mot dataangrep, administrativ programvare med mer.

4.2 Definisjon av elektronisk utstyr, kommunikasjon og lagrede opplysninger

Forskriftsforslaget inneholder definisjonen av ”Elektronisk utstyr”, ”elektronisk kommunikasjon” og ”elektronisk lagrede opplysninger”.

I følge forskriftsforslaget¹⁷ omfatter begrepet ”Elektronisk utstyr” ”*datamaskiner - herunder printere, mobiltelefoner, PDA og lignende*”. Videre at ”*Elektronisk utstyr står i motsetning til ordinært ”elektrisk utstyr” hvor behandling av personopplysninger ikke er forutsatt eller nødvendig som følge av systemet*”.

I forskriftsforslaget defineres begrepet ”Elektronisk kommunikasjon” til å ”*omfatte chatting på Internett, bruk av MSN og MMS og SMS og lignende kommunikasjonsformer som kan benyttes i dag*”. Videre at ”*løsninger for elektronisk kommunikasjon som utvikles i fremtiden er ment å skulle omfattes av forskriften*”.

¹⁶ Se <http://computer.howstuffworks.com/email.htm> vedrørende hvordan e-postsystemet fungerer

¹⁷ Se side 24 i høringsnotatet vedrørende definisjoner.

Når det gjelder ”Elektronisk lagrede opplysninger” skal disse i følge forslagforskriften ”omfatter både opplysninger som vil være omfattet av offentlighetslovens dokumentbegrep (jf. lovens § 3) og andre elektronisk lagrede opplysninger, herunder opplysninger som automatisk lagres i utstyret hver gang dette benyttes, dersom disse kan knyttes til en eller flere enkeltpersoner. Formuleringen vil blant annet fange opp dokumenter som den ansatte for eksempel har lagret på sitt hjemmeområde”.

I den videre fremstilling hvis det er behov, vil ovennevnte begrepsdefinisjoner bli lagt til grunn.

4.3 Definisjon av overvåking

Forskriftsforslaget har selv ingen definisjon på begrepet overvåking, men anviser med flere eksempler på typer av overvåking.

I følge Kunnskapsforlagets¹⁸ blå språk- og ordbokstjeneste er ordet overvåking definert som oppsyn; tilsyn: ha, holde noe(n) under oppsikt/være under oppsikt, med synonymer som bevoktning, ettersyn, kontroll, og overvåking.

I Lund-kommisjonens rapport¹⁹ definerte kommisjonen begrepet overvåking som ”*enhver kartlegging, herunder registrering av enkeltpersoner, grupper eller organisasjoner, holdninger eller virksomhet, uavhengig av måten opplysningene innhentes på og uansett hva som er grunnlaget for kartleggingen*”. Videre at ”*begrepet overvåking også har en snevrere betydning, som betegnelse på aktivt undersøkende tiltak med sikte på å holde en person, gruppe, organisasjon eller virksomhet under oppsikt. Overvåking i en slik forstand beskriver m.a.o. metoder for innhenting av informasjon*”.

Underutvalgets rapport²⁰ til arbeidslivslovutvalget definerer heller ikke innholdet i begrepet overvåking annet enn å påpeke at ”*Begrepene ”kontroll” og ”overvåking” gir gjerne assosiasjoner til tiltak som gjennomføres i arbeidsgivers interesse, og som per definisjon står i konflikt til arbeidstaker(e)s interesser*”.

¹⁸ Se <http://www.ordnett.no>

¹⁹ Innst.S.nr.240 (1996-1997) punkt 2.1.1, Innstilling fra kontroll- og konstitusjonskomiteen om rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere (Lund-rapporten).

²⁰ Underutvalgets rapport, ”Kontroll og overvåking i arbeidslivet”, avlevert 20. juni 2002 til arbeidslivslovutvalget (NOU 2004:5).

Den ”alminnelige” oppfatning²¹ av overvåking antas å være ”bli kontrollert, passet på eller bli kartlagt”. Det antas at hva som anses som overvåking kan være en subjektiv opplevelse. Arbeidsgiver kan gjennomføre tiltak som arbeidsgiver ikke anser som overvåking, mens arbeidstakeren vil kunne oppfatte tiltaket som det.

De eksemplene som er belyst i forskriftsforslaget, kan sannsynligvis tas til inntekt for det å bli kontrollert (kontrollere ansattes bruk av utstyret), og bli kartlagt (gjennomgang av logger med mer). Videre anføres det i forskriftsforslaget at ”*både den innledende kartleggingen så vel som den konkrete gjennomgangen av personopplysninger*”²² innbefattes.

Med bakgrunn i at rettskildefaktorene trekker i samme retning, defineres ordet overvåking som ”det å bli kontrollert, passet på eller å bli kartlagt”, jf også Rt. 1991/616.

4.4 Definisjon av arbeidstaker, arbeidsgiver

Forskriftsforslaget definerer ikke innhold i begrepene arbeidsgiver eller arbeidstaker, men har imidlertid flere fragmenter vedrørende forståelsen av begrepet arbeidstaker.

Personopplysningsloven inneholder ikke selv begrepet arbeidsgiver eller arbeidstaker, men bruker begrepene behandlingsansvarlig og registrert. Imidlertid tar høringen sikte på å forslå ny § 9-3 i arbeidsmiljøloven, under kapittel 9, ”Kontrolltiltak i virksomheten”, hvor det vises til gjeldende bestemmelser i personopplysningsloven med forskrifter. Ettersom forskriftsforslaget tar sikte på å regulere arbeidsgivers adgang til ansattes e-post, antas det at forskriftsforslaget legger arbeidsmiljølovens definisjon vedrørende begrepene arbeidsgiver og arbeidstaker til grunn.

I arbeidsmiljøloven § 1- 8 er arbeidstaker og arbeidsgiver definert som:

²¹ For å undersøke hvordan begrepet overvåking oppfattes ble 426 personer spurt om hva de legger i begrepet overvåking. Det er på bakgrunn av svarene den ”alminnelige” oppfatningen fremlegges. Undersøkelsen ble foretatt 6. januar 2007 – Sandvika storsenter, 109 personer, 9. januar 2007 – Oslo sentrum, 146 personer, 15. januar 2007 – Tromsø, 29 personer, og 8. februar 2007 Oslo, 142 personer. Spørsmålet som ble stilt var ”Hva forstår du med ordet overvåking?”. Det var tilfeldig forbipasserende som ble spurt, og på forskjellige tidspunkter innen samme dag. Undersøkelsen er kun gjennomført for å få en pekepinn på folks oppfatning, og kan ikke tas som inntekt for noe vitenskaplig fortolkning eller metodikk som ligger bak undersøkelsen.

²² Se side 24 i høringsnotatet.

(1) Med arbeidstaker menes i denne lov enhver som utfører arbeid i annens tjeneste.

(2) Med arbeidsgiver menes i denne lov enhver som har ansatt arbeidstaker for å utføre arbeid i sin tjeneste. Det som i denne lov er bestemt om arbeidsgiver, skal gjelde tilsvarende for den som i arbeidsgivers sted leder virksomheten.

Dertil har man inkluderende regel i arbeidsmiljøloven § 1-6, ”Personer som ikke er arbeidstakere”. I denne slås det fast at de kategorier som er opplistet er å anse som arbeidstakere i forhold til lovens regler om helse, miljø og sikkerhet når de utfører arbeid i virksomhet som går inn under loven.

Spørsmålet blir om innsyn og tilgang til ansattes e-post også kan rubriseres under helse og miljø, eller om man bare skal se hen til objektive kriteria. Hvis man bare ser hen til de objektive kriteria, vil for eksempel vernepliktige, eller personer som uten å være arbeidstakere deltar i arbeidsmarkedstiltak, jf arbeidsmiljøloven § 1-6, 1 ledd, bokstav a og g, falle utenfor arbeidstakerbegrepet i forhold til forskriftsforslaget.

Høringen har, som tidligere nevnt, noen fragmenter vedrørende arbeidstakerdefinisjonen. Bl.a. står det at ”Innsyn i e-post og annen overvåking av elektronisk kommunikasjon vil ofte kunne være del av personalsaker eller inngå som ledd i konflikter mellom arbeidsgiver og ansatte. Det er derfor ikke hensiktsmessig å avgrense mot behandling i personalsaker eller HR-sammenhenger²³”.

Videre at ”Andre som utfører arbeid for arbeidsgiver kan for eksempel være vikarer som er ansatt i vikarbyrå, konsulenter, praktikanter og lignende. Det avgjørende er at det foreligger et over- og underordningsforhold mellom arbeidsgiver og ansatt, eventuelt mellom oppdragsgiver og den som utfører oppdraget, som gir et behov for vern mot overvåking og kontroll²⁴”.

²³ Se side 24 i høringsnotatet.

²⁴ Se side 24 i høringsnotatet.

Holdt dette opp mot at forskriftsforslaget også spesifikt inkluderer elever og studenter, frivillige og tillitsvalgte i foreninger og organisasjoner, taler det for at man også inkluderer de grupper som er nevnt i arbeidsmiljøloven § 1-6.

Ut i fra at flere rettskildefaktorene trekker i samme retning, legges det til grunn ved tolkning av arbeidsgiver og arbeidstaker at det er avgjørende om det foreligger et over- og underordningsforhold mellom partene. Det er denne definisjonen vedrørende arbeidstaker og arbeidsgiver som legges til grunn i den videre fremstilling.

4.5 Definisjon av elever og studenter, frivillige og tillitsvalgte med mer

I følge forskriftsforslaget likestilles elever og studenter med ansatte²⁵. Begrunnelsen i forslagforskriften for dette er at *”fordi lærestedet for alle praktiske formål er å anse som deres arbeidsplass. Den samme type over- og underordningsforhold består mellom lærested (eventuelt representert ved rektor eller en lærer) og studenten eller eleven som mellom arbeidsgiver og ansatt”*.

Når det gjelder frivillige og tillitsvalgte i foreninger og organisasjoner²⁶ likestilles også disse *”med ansatte når disse benytter utstyr som er satt til deres disposisjon som frivillig eller tillitsvalgt”*.

Videre har høringen en setning om at *”Bestemmelsene gjelder derfor ”kun så langt de passer” på disse forholdene”*. I forhold til forskriftsforslaget § 9-1, 3. ledd, er det usikkert om dette refererer seg kun til frivillige eller tillitsvalgte, eller om de også refererer til studenter og ansatte.

Sett dette i sammenheng med merknad til bestemmelsen, og argumentasjonen som føres i høringen, antas det at begrepet *”så langt de passer”* kun refereres til frivillige og tillitsvalgte. Det er denne forståelsen som også legges til grunn i den videre fremstillingen.

²⁵ Se side 25 i høringsnotatet.

²⁶ Se side 25 i høringsnotatet.

5. Kjernepunkter i forskriftsforslaget

Grensene mellom arbeid og fritid har blitt betydelig vevd inn i hverandre, og rettstilstanden på området er uklar. Med utgangspunkt i dette og den endrede samfunnssituasjonen, ønsker høringen, og forskriftsforslaget i medhold av denne, å gi en avklaring på rettstilstanden innenfor dette området. Forskriftsforslaget prøver å regulere ”arbeidsgivers innsyn i arbeidstakers e-post og annen bruk av elektroniske virkemidler på arbeidsplassen²⁷”.

Bakgrunnen for dette er i følge høringen å gi ”vern mot innsyn i IT-verktøy som arbeidsgiver har stilt til arbeidstakers disposisjon²⁸”. Forskriftsforslagets nedslagsfelt blir dermed å gi arbeidstakerne et vern mot innsyn i de IT-verktøyene som arbeidsgiveren stiller til disposisjon i forbindelse med et arbeidsforhold.

De virkemidlene som man ønsker å bruke er personopplysningslovene ved å karakterisere kommunikasjonen med elektroniske media som personopplysninger. Videre ved å sette noen skranker ved arbeidsgivers styringsrett med utgangspunkt i personvern. Og man vil erkjenne at en arbeidstaker har en privat sfære på jobben fullt ut i fra menneskerettshensyn. For å oppnå formålet er overtredelse av reglene forbundet både med overtredelsesgebyr og straff.

I punkt 8, ”Rettslig utgangspunkt og betraktninger”, vil de tre faktorene nevnt ovenfor gjennomgås i forhold til hjemmelsgrunnlaget.

6. Nordisk rett

Sverige eller Danmark har ingen særskilte bestemmelser om arbeidsgivers innsynsrett. Innsynsretten i disse land, også når det gjelder e-post, følger de vanlige bestemmelsene om behandling av personopplysninger. Det finnes imidlertid noen vedtak fra Datainspektionen²⁹ om innsyn i e-post. Disse som har likehetstrekk med personopplysningsloven og avgjørelser fra Datatilsynet.

I Sverige er spørsmålet om regulering av vernet av personlig integritet i arbeidsforhold utredet i Integritetsutredningen, SOU 2002:18³⁰. I utredningen vurderes behovet for lovregulering og

²⁷ Se side 1 i høringsnotatet.

²⁸ Se side 1 i høringsnotatet.

²⁹ Se <http://www.datainspektionen.se/> for mer informasjon

³⁰ Se <http://www.regeringen.se/sb/d/108/a/2166>

andre tiltak for å styrke vernet av den enkeltes integritet i arbeidslivet. Utvalget la også frem et forslag til lov om vern av personlig integritet i arbeidslivet (lag om skydd för personlig integritet i arbetslivet). Bakgrunnen for lovforslaget var ifølge utredningen at det ikke fantes noen samlet regulering av vernet for personlig integritet i arbeidslivet i Sverige, og at et akseptabelt rettslig bindende vern for arbeidstakers integritet var savnet. Det blir henvist til at det nasjonalt og internasjonalt råder bred enighet om at respekt for den enkeltes privatliv og vernet av personlig integritet er en menneskerettighet som staten har plikt til å garantere gjennom lov.

Denne utredningen førte imidlertid ikke frem, og det er vedtatt at utredningen skal gjøres på nytt i Sverige³¹. Begrunnelse for dette er ”*Europeiska kommissionen deklarerade redan 2002 att det behövdes EG-direktiv om integritetsskydd i arbetslivet, men har hittills inte lyckats lägga fram något förslag*”. Og at ”*Ämnet är alltför kontroversielt*”. Den nye utredningen skal ledes av ”*Cathrine Lilja Hansson, ordförande i Arbetsdomstolen, [og] ska utreda och föreslå en svensk lagreglering för den personliga integriteten i arbetslivet*”.

Finland har en egen lov om integritetsvern i arbeidslivet (Lag om integritetsskydd i arbetslivet 13.8.2004/759³²). Loven gir generelle bestemmelser om behandling av personopplysninger. I tillegg til egne bestemmelser om innsyn og åpning av e-post tilhørende arbeidstaker, jf kapitel 6. Det er også gitt bestemmelser om samarbeide og teknisk overvåking av datanettverk, jf kapitel 7.

I korthet går den finske loven ut på at arbeidsgiver bare har rett til innsyn i e-post dersom virksomheten har tatt de nødvendige skritt for å sikre e-post. Herunder at arbeidsgiver har lagt til rette for at ansatt kan benytte automatisk fraværassistent, eller automatisk videresending av e-post ved fravær. Eller at ansatt samtykker i at en annen person kan motta e-post i dennes fravær, jf kapitel 6, §§ 18, 19 og 20.

Videre er retten til innsyn i e-postkasser bl.a. begrenset til situasjoner der det er åpenbart at ansatt har sendt eller mottatt beskjeder som, sett hen til den ansattes oppgaver og løpende saker, tilhører arbeidsgiveren. I tillegg til flere skjønnsmessige vilkår, skal gjennomføring av innsyn dokumenteres i en rapport. Denne skal fremlegges for ansatt uten unødvendig opphold.

³¹ Se <http://www.arbetslivsinstitutet.se/euarb/06-2/03.asp>, EU & arbetsrätt 2 2006.

³² Se <http://www.finlex.fi/sv/laki/ajantasa/2004/20040759>

I høringen anføres det at forskriftsforslaget på en del områder har likheter med den finske loven. Men det er viktig å anmerke at den finske loven ikke benytter ordet e-postkasse, men bruker ”e-postmeddelanden”, og ligner kanskje mer på forslaget til arbeidsutvalget³³, men med mer detaljregulering enn det arbeidsutvalget la opp til.

7. Gjeldende rett vedrørende personopplysninger

Som tidligere anført, i forhold til arbeidsgivers innsyn i arbeidstakers e-post og annen bruk av elektroniske virkemidler på arbeidsplassen, finnes det lite rettspraksis som omhandler denne problemstillingen direkte. De sakene som har vært oppe har omhandlet bevisavskjæring, jf her for eksempel Høyesteretts kjennelse av 22. november 2002, RT 2002 s. 1500, og RG 2004 s. 347, jf Rt 2003 s. 1266.

I forhold til e-post, tas RT 2002, s. 1500 i høringen³⁴ til inntekt for at det er ”*fastslått at innsyn i e-post innebærer behandling av personopplysninger og dermed faller inn under personopplysningens virkeområde*”.

Saken gjaldt spørsmålet om e-post sendt til og fra arbeidstakers e-postadresse hos arbeidsgiver, uten arbeidstakerens samtykke kunne fremlegges som bevis i avskjedssak. Kjæremålsutvalget kom til at arbeidsgiver har rett til innsyn i virksomhetsrelatert e-post og at lagmannsretten ikke hadde tolket personopplysningsloven § 8 bokstav f feil.

Selv om saken i utgangspunktet gjaldt primært de ulovfestede reglene om bevisavskjæring, tar den opp en interessant problemstilling i forhold til e-post.

Bl.a. sies det at ”*Kjæremålsutvalget vil bemerke at forutsetningen for at personopplysningsloven overhodet skal kunne anvendes på X AS' fremgangsmåte i denne saken, er at e-postmeldingene kan karakteriseres som personopplysninger i lovens forstand, jf. lovens § 2 nr. 1*”.

Videre er Kjæremålsutvalget enige i drøftelsen til lagmannsretten;

³³ NOU 2004: 5 Arbeidslivslovsutvalget

³⁴ Se side 4 i høringsnotatet.

”Ut fra de foreliggende opplysninger legger lagmannsretten til grunn at alle meldingene gjelder aktiviteter, spørsmål, planer o.l. som på en eller annen måte har forbindelse med den type virksomhet som X står for eller er interessert i. I et slikt perspektiv er det ikke grunn til å oppfatte meldingene som private”.

Videre *”Lagmannsretten viser for øvrig til opplysningene om hvordan A har angitt avsender på meldingene, og nøyer seg med å konstatere at meldingene med minst like stor rett kan hevdes å være virksomhetsrelaterte som private. På denne bakgrunn er det ikke grunnlag for å konstatere at bevisene er fremskaffet på lovstridig måte”.*

Videre sies det at *”Lagmannsretten har knyttet sin drøftelse til karakteristikken ”virksomhetsrelatert”. Dette er et begrep som ikke brukes i personopplysningsloven. De elementer som lagmannsretten i denne forbindelse legger vekt på, er imidlertid dekkende i forhold til vurderingen etter § 8 bokstav f, jf. dens krav om ”berettiget interesse””.*

Utvalget viser for øvrig også til Datatilsynets hjemmeside, hvor det heter: *”Kan arbeidsgiveren lese e-posten min?”*³⁵

Også RG 2004 s. 347 være illustrerende. RG 2004 s. 347 gjaldt en sak om oppsigelse hvor arbeidsgiver fremla oversikt over filer innhentet fra en bærbar pc som arbeidsgiver hadde stillet til arbeidstakers disposisjon for arbeidet. Lagmannsretten fant at beviset var fremskaffet i strid med personopplysningsloven og derfor ulovlig, men at det likevel ikke skulle avskjæres som bevis. Hensynet til sakens opplysning og den frie bevisbedømmelse måtte veie tyngre enn personvernens hensynet.

Lagmannsretten uttaler at *”Når det da ikke foreligger noen avtale om slik kontroll, intet samtykke, ingen interne retningslinjer eller instruksjoner som var kjent for arbeidstageren, ser lagmannsretten det slik at interesseavveiningen må slå ut til fordel for personvernet for den ansatte. Dette syn bestyrkes av at det program som var gjenstand for undersøkelse, var et*

³⁵ ”Kan arbeidsgiveren lese e-posten min? Det er viktig å skille mellom privat og virksomhetsrelatert e-post. Arbeidsgiveren din har ikke adgang til å lese e-post du mottar som privatperson uten at du har samtykket. Dette gjelder selv om arbeidsgiveren må sies å være ”eier” av datasystemet. Arbeidsgiveren har imidlertid rett til innsyn i virksomhetsrelatert e-post. Arbeidsgiverens interesse i å lese disse meldingene overstiger hensynet til ditt personvern”.

internettprogram registrert i As navn og at det fremgikk tydelig av filene at de var av rent privat karakter.”

I sin vurdering har lagmannsretten lagt vekt på at arbeidsgiveren kunne ha sørget for å fjerne enhver tvil om adgangen til privat bruk, gjennom avtale eller instruks i forbindelse med at PC-en ble stilt til disposisjon. Det er videre lagt vekt på at arbeidsgiver, dersom han mente at det ble brukt private abonnement i strid med avtale eller i strid med arbeidsgivers interesse, kunne ha pålagt alle å fjerne slike private abonnement og private filer. Videre ble det vektlagt at det ville ha vært et langt mindre integritetskrenkende inngrep enn å gå inn i de filer som var klart angitt som private - og at det ville ha vært et tilstrekkelig inngrep for formålet.

Selv om de to ovennevnte sakene inneholder personvern vurderinger, omhandler de som nevnt primært de ulovfestede reglene om bevisavskjæring. Det er derfor usikkert om man kan legge avgjørende vekt på disse ut fra et personvernperspektiv.

Selv om det finnes flere tilsvarende avgjørelser³⁶, har spesielt næringslivet ønsket en avklaring på disse spørsmål. Datatilsynet³⁷ har forholdt seg til sine egne retningslinjer³⁸ og gitt en rekke enkeltvedtak med utgangspunkt i disse. Mange av vedtakene har blitt angrepet rettslig og utfallet av påtalemyndighetens etterfølgende prøving har variert³⁹. Rettstilstanden er derfor fortsatt usikker på dette området.

7.1 Datatilsynets retningslinjer

Som tidligere nevnt er rettssituasjon uavklart på dette området. Datatilsynet har imidlertid gitt retningslinjer på hvordan dette området er å forstå⁴⁰. Hvilken rettskildemessig vekt og relevans slike alminnelige retningslinjer skal eller bør tillegges, vil kunne avhenge av flere faktorer.

³⁶ Se for eksempel 2001/1589 og RG 2003/707.

³⁷ Personopplysningsloven § 42 gir hjemmel til Datatilsynets oppgaver.

³⁸ Se http://www.datatilsynet.no/templates/article____201.aspx

³⁹ Datatilsynets anmeldelse av Redningsselskapet, saken ble henlagt av statsadvokaten i september 2006. Vedtaket ble klaget inn for Riksadvokaten i oktober 2006 med etterfølgende henleggelse. Datatilsynets anmeldelse av Vinmonopolet AS i oktober 2005. Denne ble henlagt av august 2006. Anmeldelse av Bazar Forlag i juli 2006. Se <http://www.datatilsynet.no> for mer informasjon om disse sakene.

⁴⁰ Se www.datatilsynet.no under fanen e-post.

I forhold til relevans skal Datatilsynet etter personopplysningsloven § 42, 3. ledd, nr. 5 ”identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses”. Og etter personopplysningsloven § 42, 3. ledd nr. 6, ”gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder bistå i utarbeidelsen av bransjevise atferdsnormer”.

Ses dette i forhold til forvaltningsloven § 11, har Datatilsynet en alminnelig veiledningsplikt innenfor sitt saksområde. Med bakgrunn i dette, kan det antas at rettskildemessig relevans i forhold til Datatilsynets retningslinjer er avklart.

Det andre forholdet vil være hvilken vekt Datatilsynets retningslinjer skal tillegges. På et generelt grunnlag i forhold til rettskildelære vil en retningslinje ha større vekt hvis flere rettskildefaktorer peker i samme retning, og motsatt hvis de spriker innbyrdes.

Med utgangspunkt i sine egne retningslinjer har Datatilsynet gitt enkeltvedtak. Det vil kunne skape presedens om disse blir stående og fulgt i senere avgjørelser, spesielt hvis dem det angår også oppfatter dette til å være gjeldende rett. Motsatt vil det være om vedtaket blir etterprøvd og endret, for eksempel i klageomgangen, høyere forvaltningsorgan eller av påtalemyndighet.

Personvernemnda, som er i følge personopplysningsloven § 43 klageinstans for Datatilsynets avgjørelser, har ikke vært fremlagt spørsmål om innsyn i e-post. Påtalemyndigheten har henlagt Datatilsynets anmeldelser av Redningsselskapet og Vinmonopolet. Videre er det uenighet om Datatilsynets retningslinjer i næringslivet, og da spesielt i forhold til arbeidsgivers styringsrett. Høyesterett har heller ikke tatt eksplisitt stilling til hvilken rettskildemessig vekt Datatilsynets retningslinjer har, bortsett fra å referere til disse i Rt 2002 side 1500. Men her uttalte også Høyesterett at arbeidsgiver hadde rett til innsyn i virksomhetsrelatert e-post, og brukte heller ikke begrepet e-postkasse.

Sett i forhold til det ovennevnte antas det at Datatilsynets retningslinjer har en svekket rettskildemessig vekt, og man må falle ned på mer generelle betraktninger. Derfor vil det være behov for å kodifisere gjeldende rett for å avklare rettstilstanden, noe også høringen legger opp til.

7.2 Gjeldende rett vedrørende e-post spesielt

Som tidligere nevnt, består e-post av tre komponenter; selve meldingen, e-postadressen (for eksempel per.person@virksomhet.no), og e-postkassen (@virksomhet.no som kan sammenliknes med ordinær postkasse). I dette avsnittet ses det på de tre komponentene i forhold til gjeldene rett.

Tar man utgangspunkt i selve meldingsinnholdet, er det både i juridisk teori og praksis antatt at det kan karakteriseres som personopplysning, jf bl.a. Rt. 2002 side1500;

”Kjæremålsutvalget vil bemerke at forutsetningen for at personopplysningsloven overhodet skal kunne anvendes på X AS' fremgangsmåte i denne saken, er at e-postmeldingene kan karakteriseres som personopplysninger i lovens forstand, jf. lovens § 2 nr. 1”.

Når det gjelder selve e-postadressen (for eksempel per.person@virksomhet.no) er det også antatt at selve opplysningen, her for eksempel per.person@virksomhet.no, i lovens forstand er en personopplysning. Dette kan utledes direkte av personopplysningsloven § 2, 1. ledd nr 1) hvor personopplysning definert som ”opplysninger og vurderinger som kan knyttes til en enkeltperson”, og personverndirektivet artikkel 2, bokstav a.

Tar man et formelt teknologisk utgangspunkt i e-postkassen, kan den best forklares med en analogi til tradisjonell brevforsendelse. Tenker man seg at person A sender et brev til person B i virksomhet B, går brevet gjennom Posten og havner i virksomhet Bs postkasse. Det er viktig å legge merke til at Posten ikke leverer brevet direkte til B (vi ser bort i fra rekommanderte brev og punkt til punkt spesialsendinger) men at den havner i den ”store” virksomhetspostkassen. Fra denne kassen sorteres brevene for eksempel av dokumentsenderet, arkivet eller postmottaket, for deretter å videreformidle brevet til den enkeltes interne postkasse.

Tilsvarende er det når A sender en e-post til B i virksomhet B. E-posten går gjennom forskjellige servere og noder⁴¹ (i tradisjonell forstand vil dette være ”Posten”) og kommer frem til virksomhetens postkasse, dvs @virksomhet.no (dvs den ”store”

⁴¹ Noder kan for eksempel være rutere som ruter internettrafikken, spam-systemer, mellomlagring og andre tekniske innretninger for å påse at data fra punkt A kommer korrekt frem til punkt B.

virksomhetspostkassen i tradisjonell brevhåndteringssystem). Man sender altså ikke e-post direkte fra person til person, men fra server til server, i dette tilfellet vil mottaksserveren være @virksomhet.no.

Pga. Internetts natur vil det kunne ligge flere begrensninger for å ivareta sikkerhet i e-postsystemet. E-posten kan automatisk bli lest av spamfiltre for å fjerne ”søppelpost”, innholdet kan bli lest av viruskannere, og man kan også lese e-posten manuelt hvis en av de andre tekniske mekanismene som er implementert slår ut⁴² av ulike årsaker. På e-postserveren ligger det interne e-postkasser (for eksempel per.person@), hvor e-posten fra A sendes etter at alle interne tekniske eller manuelle kontroller er foretatt.

Som man kan se tjener e-postadressen to formål; det ene er å identifisere e-postkassen til en person, og det andre er at det er en e-postkasse i seg selv. Hvis man antar at e-postadressen er per.person@virksomhet.no, og overfører det til tradisjonell brevhåndtering, vil Per Person være teksten som står på den interne postkassen (eller kontoret) hvor den vanlige posten leveres.

At selve opplysningen per.person@virksomhet.no i seg selv er personopplysning er ikke bestridt, ettersom den også i lovens forstand anses som en personopplysning. Men det som er uklart er om den andre funksjonen, dvs at opplysningen også er en postkasse, om denne funksjonen også er en personopplysningen og kan innfortolkes i personopplysningsloven.

Denne problemstillingen har ikke vært behandlet i rettspleien. Innenfor juridisk teori har dette spørsmålet fått større aktualitet den siste tiden. Datatilsynet har gjennom sine anbefalinger og retningslinjer⁴³ samt høringsnotatet, imidlertid tatt utgangspunkt i at arbeidsgiver ikke har rett til innsyn i en persons e-postkasse. Hjemmelgrunnlaget for dette vil bli diskutert under punktet ”Rettslige betraktninger”.

⁴² Det vil føre for langt å gå inn på alle tekniske mekanismer som finnes, både manuelle og automatiserte, i mellomfasen fra e-posten kommer inn i hovedpostkassen, for eksempel @virksomhet.no til den faktisk når mottakeren i virksomheten.

⁴³ Se <http://www.datatilsynet.no>, under arkfanen e-post.

Høringsnotatet bruker også ordene ”Enhver form for gjennom søkning, åpning eller lesing av e-post og overvåkning av elektronisk utstyr er å anse som behandling av personopplysninger jf. personopplysningslovens § 2 nr. 2”⁴⁴.

Ordet ”Enhver” antas å forstås dit hen at det gjelder kun opplysninger som kan knyttes til en person i datasystemet eller i datanettverket. Dette er begrunnet med at i et datanettverk utveksles det også mye annen informasjon eller data som ikke er personrelatert. Man kan for eksempel tenke seg at flere brukere deler en datamaskin, og at denne er i et datanettverk hvor systemansvarlig kan kjøre forskjellige typer av ”ping-kommando”⁴⁵. Et annet eksempel kan være enheter som kun måler belastning på datanettverket. Denne informasjonen vil vanskelig kunne sies å være personrelatert ettersom den ikke vil kunne inneholde ”personopplysninger”.

Høringsnotatet er selv inne på dette hvor det sies ” Forskriften skal ikke gjelde ved enhver behandling av personopplysninger som er nødvendig i et ansettelsesforhold”, og ”Det er derfor avgrenset til arbeidsgivers gjennom søkning, åpning eller lesing av e-post og overvåkning av elektronisk utstyr”⁴⁶.

Men sett i forhold til formålet med personopplysningsloven, legges det til grunn at forskriftsforslaget her sikter til informasjon i datanettverket som kan relateres til en person, og ikke all informasjon som flyter i et datanettverk. Det er også denne forståelse som videre legges til grunn.

Det er utvilsomt at personrelatert informasjon som flyter i datanettverket vil kunne omfattes av personopplysningsloven § 2, og spesielt e-post.

Selv om de sakene som har vært oppe til vurdering i rettspleien har dreid seg om bevisavskjæring, kan de til en viss grad gi veiledning. Men det er uklart hvilken rettsstilstand som egentlig gjelder på dette området, spesielt gjelder det i forhold til innsyn i e-postkasser. Og det virker som om man må falle tilbake på de generelle vurderinger i forhold til

⁴⁴ Se side 23 i høringsnotatet.

⁴⁵ En ”ping-kommando” er en nettverkskommando for å se om en datamaskinen ”eksisterer” i nettverket, og for å måle hastigheten av datatransmisjonen mellom maskin A og B.

⁴⁶ Se side 24 i høringsnotatet.

kontrollformål, arbeidsgivers styringsrett og personvern hensyn, jf punktet ”Personvern på arbeidsplassen, arbeidsmiljøloven”.

8. Forskriftsforslaget nedslagområdet

Utgangspunktet for Datatilsynet har vært å rubrisere både e-post og kommunikasjon ved hjelp av IT-verktøy som personopplysning. Ettersom forskriftsforslaget tar sikte på å regulere forhold i arbeidslivet, gjennomgås først menneskerettigheter og EØS-rett. Deretter kort om personvern på arbeidsplassen, samt forhold til annen lovgivning.

8.1 Menneskerettigheter og EØS-rett

Et sentralt poeng for forskriftsforslaget er retten til privat sfære på arbeidsplassen med begrunnelse i bl.a. menneskerettigheter og EØS-lovgivningen, og som er inkorporert i norsk rett. Med bakgrunn i dette anfører at man kan innskrenke arbeidsgivers adgang til ansattes e-post.

Norge er forpliktet av flere internasjonale avtaler vedrørende vernet av den personlige integritet. Blant de mest sentrale er Den europeiske menneskerettighetskonvensjon av 4. november 1950, Europarådskonvensjon nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger, og EUs personverndirektiv.

Disse reglene har direkte eller indirekte betydning for spørsmålet om regulering av adgangen til kontrolltiltak. Menneskerettighetskonvensjonene er inkorporert i norsk rett gjennom menneskerettsloven, og personverndirektivet via personopplysningsloven.

Den europeiske menneskerettighetskonvensjon (EMK)⁴⁷ artikkel 8 nr. 1 slår fast at:

”Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.”

Bestemmelsen beskytter retten til privatliv, som er retten til å leve sitt liv uten inngripen fra utenforstående. Dette omfatter rett til så vel fysisk og psykisk integritet, som beskyttelse av ære og rykte. Retten til privatliv omfatter også beskyttelse mot overvåking og beskyttelse av informasjon om private forhold.

⁴⁷ EMK artikkel 8 nr. 1 er utdypet i NOU 2004: 5 *Arbeidslivslovsutvalget*.

Artikkel 8 er en tolkningsfaktor i forhold til personopplysningsloven. Dette følger av at konvensjonen gjelder direkte som norsk lov, jf menneskerettsloven § 2.

Videre beskytter FN-konvensjonen om sivile og politiske rettigheter, artikkel 17, også den personlige integritet:

1. *Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.*
2. *Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.*

Også denne konvensjonen er gjort til norsk lov gjennom menneskerettsloven.

I utgangspunktet setter disse bestemmelsene skranker for staten i forhold til enkeltindividet. Spørsmålet er om bestemmelsene også setter skranker i forholdet mellom private, typisk i forholdet mellom arbeidsgiver og arbeidstaker, dvs konvensjonenes horisontale effekt.

Europadomstolen har uttalt at staten har en viss plikt til å beskytte private mot andres overtredelse av deres privat- og familieliv. Domstolen har imidlertid ikke tatt stilling til om dette også gjelder i forholdet mellom private.

Den Europeiske Menneskerettighetsdomstol (EMD) har behandlet flere saker som angår artikkel 8, og to avgjørelser som kan nevnes her er Niemietz⁴⁸ mot Tyskland, og Halford⁴⁹ mot Storbritannia.

Det kan også nevnes at en avgjørelse i den svenske Arbetsdomstolen i en dom fra 1998 kom til at narkotikatesting av ansatte ved et atomkraftverk ikke var i strid med artikkel 8⁵⁰.

⁴⁸ I Niemietz-saken hadde offentlige myndigheter gjennomført klagers kontor, noe klager anførte at krenket hans rett etter EMK artikkel 8. Myndighetene på sin side anførte at artikkel 8 ikke ga beskyttelse mot gjennomføring av en persons kontor, på bakgrunn av konvensjonens skille mellom privatliv og hjem på den ene siden, og arbeidsliv på den andre. Myndighetenes anførsler førte ikke frem. EMD fremholdt at det ikke var grunnlag for å tolke "privatliv" så snevert at det utelukket aktiviteter på arbeidsplassen.

⁴⁹ I Halford fant EMD at kontroll av telefonsamtaler som ansatte fører på arbeidsplassen var en overtredelse av konvensjonens artikkel 8. Halford var ansatt i politiet, og hadde adgang til to telefoner, hvor den ene var til private formål. Det var ikke gitt noen restriksjoner eller instruksjoner om bruken av telefonene. Halford anførte at arbeidsgiver hadde avlyttet hennes telefoner med det formål å sikre seg bevis i en pågående tvist. EMD fant det klart at telefonsamtaler tatt fra kontorlokaler faller inn under "privatliv" og "korrespondanse" i artikkel 8.

Det som kan anmerkes til de ovennevnte dommene, er at sakene ikke gjaldt i forhold mellom private rettssubjekter, men i forhold mellom privatperson (ansatt) og myndighetene.

I forhold til norsk juridisk teori diskuteres det om forholdet myndighet/privat rettssubjekt i forhold til EMK artikkel 8, også kan transponeres til å gjelde private rettssubjekter.

Europarådskonvensjon nr. 108, om personvern i forbindelse med elektronisk behandling av personopplysninger fra 1981, er ratifisert av Norge. Konvensjonen gjelder all lagring og behandling av personopplysninger (personvernkonvensjonen) ved elektronisk databehandling. EUs personverndirektiv bygger på konvensjonen. Bestemmelsene gjelder som lov i Norge, jf. menneskerettsloven § 2, og går ved motstrid foran bestemmelser i annen lovgivning, jf. menneskerettsloven § 3. Personopplysningsloven ble ved vedtakelsen ansett for å være i overensstemmelse med konvensjonen.

I forhold til personopplysningsloven, sier Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995, om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger i fortalen punkt 10 at:

”De nasjonale lovgivninger om behandling av personopplysninger har som mål å verne de grunnleggende rettigheter og friheter, særlig retten til privatlivets fred, som er anerkjent både i artikkel 8 i Den europeiske konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter og i fellesskapsrettens generelle prinsipper. Derfor må tilnærmingen av lovgivningene ikke føre til en svekkelse av den beskyttelsen de gir, men tvert imot ha som mål å sikre et høyt vernnivå i Fellesskapet”.

Med bakgrunn i dette er det slått fast retten til en personlig sfære på arbeidsplassen av den Europeiske Menneskerettighetsdomstol (EMD), i medhold av den Europeiske Menneskerettighetskonvensjon (EMK) artikkel 8. Retten til respekt for sitt ”privatliv” og ”korrespondanse” er av domstolen tolket slik at det også omfatter en persons aktiviteter på arbeidsplassen og da i forhold til personverndirektivet.

⁵⁰ AD 1998 nr. 97

Dette utgangspunktet er også slått fast i prinsippavgjørelser fra Høyesterett, bl.a. i Rt. 1991/616 ("Gatekjøkkenkjennelsen"). Her avviste Høyesterett fremleggelse av et hemmelig videoopptak fra gatekjøkkenet som bevis i en arbeidstvist. De ansatte var klar over at det var montert videokamera i lokalet. Formålet med kamera var å gjøre det mulig å oppholde seg på pauserommet og samtidig få kjennskap til om det var kunder inn på gatekjøkkenet. At kameraet i perioder ble brukt til overvåking av de ansatte var ikke kjent for de ansatte og derfor i strid med formålet for ordningen. Beviset var dermed å anse som hemmelig videoopptak og kunne ikke legges til grunn. Høyesterett mente at slik hemmelig overvåking representerte et vidtgående integritetsinngrep i forhold til de ansatte, og at fremgangsmåten medførte, ut fra alminnelige personvern hensyn, at et slikt inngrep i den personlige integritet måtte anses som uakseptabelt.

Med bakgrunn i dette, slik også forskriftsforslaget legger opp til, har en arbeidstaker krav på privat sfære på arbeidsplassen.

8.2 Personvern på arbeidsplassen i forhold til arbeidsmiljøloven

Ansatte har krav på vern av sin personlige sfære på arbeidsplassen. Dette er også slått fast i prinsippavgjørelser fra Høyesterett, jf for eksempel Rt. 1991/616. Selv om det prinsipielle utgangspunktet er slått fast, gir det likevel ikke den nødvendige klarhet i forhold til ansattes bruk av e-post, og arbeidsgivers rett til innsyn i og kontroll av denne.

I forhold til ny arbeidslov⁵¹, fremmet ikke departementet regler om innsyn i e-post på bakgrunn av Datatilsynets innvendinger mot Arbeidslivslovutvalgets forslag, samt at det pågikk et arbeid med å utarbeide forskrifter om dette.

Selv om forskriftsforslaget nå er fremsatt, er det likevel grunn til kort å gå gjennom arbeidsrettslige problemstilling og gjeldende rett på området.

Temaet kontroll og overvåking i arbeidslivet dekker et vidt spekter av tiltak og problemstillinger, og aktualiserer to problemstillinger. For det første gjelder det rekkevidden av arbeidsgivers adgang til å iverksette kontrolltiltak overfor de ansatte. Og for det andre

⁵¹ Jf Ot. prp nr. 49 (2004 – 2005)

spørsmålet om adgangen til å behandle opplysninger om arbeidstakerne som fremkommer som et resultat av kontrolltiltak.

Problemstillingene omhandler i utgangspunktet to forskjellige spørsmål, samtidig som det er en nær indre sammenheng mellom disse. For eksempel inngår de overordnede personvern hensyn som ligger til grunn for personopplysningsloven, også som sentrale elementer i vurderingen av spørsmålet om selve kontrolltiltakenes rettmessighet. Men samtidig vil de være formålsløse dersom det ikke er adgang til å behandle de personopplysninger som fremkommer gjennom kontrolltiltak, for eksempel ved å lagre opplysningene om tidsregistrering, salgsresultater, eller en inventarliste med oversikt over hva en ansatt har fått utlevert av teknisk utstyr.

Kontrolltematikken representerer i utgangspunktet to interesser som ofte kan være motstridende; arbeidsgivers ønske om å iverksette kontrolltiltak på den ene siden, og vern arbeidstakers personverninteresser på den andre. Vernet av den personlige integritet er en helt vital interesse, noe som også er slått fast i rettspleien. Arbeidsgivers kontrollinteresse er imidlertid ofte godt begrunnet, og det er antatt at den kan i spesielle tilfeller gå foran personverninteressene, jf her for eksempel RG 2004 s. 347.

I arbeidsmiljøloven kapittel 9, gis det generelle overordnede prinsipp om kontroll og overvåking i arbeidslivet. ”Arbeidsgiver kan bare iverksette kontrolltiltak overfor arbeidstaker når tiltaket har saklig grunn i virksomhetens forhold, og det ikke innebærer en uforholdsmessig belastning for arbeidstakeren”⁵². Videre inneholder kapittelet bestemmelser om drøfting, informasjon og evaluering av kontrolltiltak i virksomheten, samt arbeidsgiver har plikt til å drøfte behov, utforming og gjennomføring mv av kontrolltiltak med arbeidstakernes tillitsvalgte, og at tiltakene skal evalueres jevnlig.

Arbeidsmiljøloven inneholder ikke konkrete bestemmelser om arbeidsgivers rett til innsyn i ansattes elektroniske utstyr. Det følger imidlertid av arbeidsmiljøloven § 9-1 (2) ”at Personopplysningsloven gjelder for arbeidsgivers behandling av opplysninger om arbeidstakere”.

⁵² Jf arbeidsmiljøloven § 9-1, 1. ledd.

Dermed vil man få motstridende interesser, på den ene siden hvor langt kompetansen rekker, og da spesielt i forhold til styringsretten, for arbeidsgiveren til å kunne gjennomføre kontrolltiltak, og på den andre siden arbeidstakerens personvern.

Det er gjennom rettspraksis utviklet generelle arbeidsrettslige regler og prinsipper som slår fast at kontrolltiltak skal ha saklig grunn og være forholdsmessige, jf også arbeidsmiljøloven § 9-1 (1).

Kravet til saklig grunn innbefatter en lang rekke forhold, slik som for eksempel teknologiske, økonomiske, sikkerhets-, arbeidsmiljø- og helsemessige forhold vil kunne utgjøre saklig grunn for kontrolltiltak. Saklighetskravet inneholder to elementer. Det må for det første foreligge et saklig formål bak kontrolltiltaket som er forankret i virksomheten som sådan. Videre inneholder vilkåret om saklig grunn et krav om vedvarende saklighet, jf arbeidsmiljøloven § 9-2 (3), det vil si at kontrolltiltaket må opphøre når det behov eller formål som begrunnet tiltaket ikke lenger eksisterer eller er betydelig redusert.

Ved forholdsmessighetsvurderingen er det også antatt at det ikke vil være tilstrekkelig å vurdere det enkelte tiltak for seg, men at man må se på summen av kontrolltiltak i virksomheten. Selv om et kontrolltiltak isolert sett er i samsvar med lovens vilkår, vil gjennomføringen av det kunne bli ansett som ulovlig. Dette spesielt hvis summen av eksisterende kontrolltiltak i bedriften medfører at den forsvarlige tålegrense for arbeidstakerne som sådan blir overskredet.

Vurderingen av om kontrollen vil medføre en uforholdsmessig belastning, vil kunne bero på en rekke elementer, som for eksempel tiltakets formål, kontrollens art, praktisk gjennomføring, og hvilke inngrep som foretas i arbeidstakernes personvern.

Det er ansett i rettspleien at dersom kontrolltiltaket vil medføre ikke ubetydelig inngrep i rettsgoder, som personlig integritet, verdighet, privatlivets fred, legemets ukrenkelighet eller lignende, vil vilkårene for å gjennomføre kontrollen i utgangspunktet vanskelig kunne sies å være oppfylt. Motsatt skal det mye til for at mer tradisjonelle kontrolltiltak i arbeidslivet vil bli ansett som uforholdsmessig (for eksempel tidsregistrering, adgangskontroll, salgsoversikter, resultatbasert lønn med mer).

Når det gjelder kravet om saklighet, er det i rettspleien slått fast at utøvelse av styringsretten begrenses av alminnelige saklighetsnormer. Dette kommer til uttrykk av Høyesterett i Rt. 2001 s. 418 og Rt. 2000 s. 1602. Med saklighet i denne sammenheng menes at tiltaket skal være begrunnet i forhold som vedrører virksomheten, og at tiltaket skal være egnet til å fremme formålet og ikke settes i verk vilkårlig overfor arbeidstakerne, jf også RT 2004 side 1844.

I Rt. 2000 side 1602 (såkalte Nøkksaken), fremkommer følgende generelle merknader om styringsrettens rekkevidde:

”Arbeidsgiveren har i henhold til styringsretten rett til å organisere, lede, kontrollere og fordele arbeidet, men det må skje innenfor rammen av det arbeidsforhold som er inngått. Ved tolkningen og utfyllingen av arbeidsavtalene må det blant annet legges vekt på stillingsbetegnelse, omstendighetene rundt ansettelsen, sedvaner i bransjen, praksis i det aktuelle arbeidsforhold og hva som finnes rimelig i lys av samfunnsutviklingen.”

Dette ble senere fulgt opp i Rt. 2001 side 418 (såkalte Kårstø-dommen). Saken gjaldt spørsmålet om hvor på området arbeidstakerne måtte være ved arbeidstidens begynnelse og slutt i forbindelse med at arbeidsgiver hadde gjennomført endringer i arbeidstakernes fremmøtested.

Under henvisning til de ovenfor siterte Rt 2000 side 1602 uttalte retten at:

”Det følger av styringsretten at Statoil innenfor de rammer lovgivningen og avtaler oppstiller, har rett til å fastsette det fremmøtested hvor arbeidstakerne skal stå til disposisjon for å utføre arbeidsoppgavene.”

Høyesterett konkluderte slik:

”De endringer som er gjennomført, må anses å ligge innenfor rammen av arbeidsforholdet. Etter min mening er endringene samlet sett ikke så omfattende at de går ut over det arbeidsgiver kan foreta i kraft av styringsretten som en restkompetanse.”

Når det gjelder kravet om forholdsmessighet, skal det foretas en avveining mellom arbeidsgivers interesse i kontrolltiltaket og arbeidstakerens personvern. Det skal tas hensyn til hvor inngripende tiltaket er eller kan bli for den enkelte, samt generell respekt for verdighet og privatliv. Hensynet til personlig integritet er tillagt vekt av Høyesterett i flere saker, og rettspraksis må sies å være et uttrykk for de samme prinsipper som er nedfelt i EMK artikkel 8.

Med bakgrunn i dette er det antatt at arbeidsgiver kan, med bakgrunn i styringsretten, gå forholdsvis langt når det gjelder å ivareta arbeidsgiverens legitime interesser. Dette spesielt der kontrolltiltaket ikke krenker de helt vitale personlige interesser.

Sett opp i mot at arbeidstaker har krav på vern av sin personlige sfære på arbeidsplassen, vil innhold i dette vernet avhenge av rekkevidden til styringsretten sett opp i mot hvilken personlig krenkelse kontrolltiltaket er ovenfor arbeidstakeren.

I forhold til forskriftsforslaget innebærer det at arbeidsgiver kan gå forholdsvis langt når det gjelder kontrolltiltak i kraft av sin styringsrett. Videre at arbeidstaker må respekter arbeidsgivers innsynsrett i forhold til å ivareta virksomhetens legetime interesser. Men kan ikke innsynsretten være av en slik art at den er utilbørlig ovenfor ansatte.

8.3 Postloven og arkivloven

Avsender i en meldingsbasert kommunikasjonstjeneste som e-post, kan ha en forventning om at denne behandles på samme måte som tradisjonell brevpost. Dette kan for eksempel gjelde i forbindelse med reklamasjon, purringer eller avtaleinngåelse.

I postlovens § 9, første ledd, beskrives det at *"Avsender av postsending har råderett over postsendingen til den er utlevert til mottaker på bestemmelsesstedet"*. Videre kommer dette prinsippet igjen til uttrykk i arkivforskriftens § 3-2.

Selv om postloven regulerer et annet forhold, er det interessant å trekke en analogi i forhold til ovennevnte problemstilling. Og tilsvarende i forhold til arkivforskriftens § 3-1, 2. ledd, reguleres forholdet til personlig adressert post. Dvs der navnet til mottaker står foran virksomhetens navn. Det er hjemlet at brevet skal leveres uåpnet til mottaker, såfremt det ikke er inngått en avtale med mottaker om åpning av slike brev.

I forhold til e-post blir det da spørsmål om e-postadressen, for eksempel per.person@virksomhet.no, kan anses som personlig (navnet til personen står foran @virksomhet.no), eller om det er en teknisk innretning for å i det hele tatt kunne levere e-post til virksomheten. Anses e-postadressen som personlig vil forholdet kunne reguleres av arkivforskriften § 3-1, 2. ledd. Og motsatt, at det er en virksomhetsadresse, vil i så fall forholdet kunne reguleres av arkivforskriften § 3-1, 1. ledd, jf 3. ledd, første punktum.

Disse spørsmål har ikke vært til behandling i rettspleien og også vært lite behandlet av juridisk teori. Avklaring av dette vil også være interessant i forhold til innsynsretten for arbeidsgiver.

For hvis det er slik at det er virksomhetsnavn som står først (dvs at @virksomhet er å tolke at denne kommer før per.person@) vil arbeidsgiver kunne se all e-post som kommer inn til virksomheten som virksomhetsrelatert e-post og kunne deretter sortere ut privat e-post, jf arkivforskriften § 3-1. Ser man hen til hvordan e-post teknisk fungerer, vil dette sannsynligvis la seg vanskelig gjennomføres i praksis. Dette fordi alt går inn i en e-postkasse, og hvis ikke den private e-posten er kryptert, vil arbeidsgiver i motsetning til private brev (vi ser bort i fra postkort) kunne se innholdet, og dermed vil ikke formålet med å beskytte arbeidsgivers private sfære være oppfylt.

8.4 Strafferett

Straffeloven § 145 inneholder bestemmelser om brevbrudd og om uberettiget adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske virkemidler.

Straffelovens § 145;

”Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder eller begge deler.

Det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.

Voldes skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.

Medvirkning straffes på samme måte.

Offentlig påtale finner bare sted når allmenne hensyn krever det.”

Det er nevnt flere hensyn bak straffelovens § 145 i NOU 1985:21, Datakriminalitet. Det vises spesielt til hensynet til privatlivets fred og behovet for vern mot uberettiget utnyttelse av informasjon. Private områder som er skjermet mot innsyn kan også bidra til å fremme privatlivets fred. I korthet betyr det at man kan oppbevare sine elektroniske data, som for eksempel musikkfiler, filmer, programmer, dokumenter og e-post, på områder som er skjermet for innsyn fra andre.

Privatlivets fred er fundamentale menneskerettigheter som myndighetene plikter å sikre borgerne, jf EMK art 8 og menneskerettsloven § 2. Straffeloven § 145, 2. ledd, jf straffelovens § 145 a, skal bidra til å effektivisere denne forpliktelsen. Bestemmelsen verner om personvernet og har til dels samme nedslagsområde som personopplysningsloven.

Subjektet for straffeansvar vil normalt kunne være forskjellig ved overtredelse av straffelovens § 145, 2. ledd og personopplysningsloven. Dette fordi personopplysningsloven hjemler straffesanksjonerte plikter for dem som behandler personopplysninger, jf personopplysningsloven § 48, mens straffeloven § 145, 2. ledd, setter straff for dem som ”uberettiget skaffer seg adgang til data, herunder også personopplysninger”.

Det er også slik at straffelovens § 145, 2. ledd, verner mot uberettiget adgang til ubeskyttede data, og det forlanges at en tredjeperson respekterer dataenes konfidensialitet og integritet selv om de teknisk sett vil kunne være tilgjengelige for vedkommende.

Problemstillingen vil da kunne knyttes til ”uberettiget skaffer seg adgang” i forhold til arbeidsgiver. Det innebærer at bestemmelsen kun kommer til anvendelse når gjerningspersonen er materielt sett uberettiget til dataene. Berettigelsen for uberettigelse må avgjøres på grunnlag av andre normer utenfor straffelovgivningen, dvs for eksempel instruks, lovverk, avtaler eller retningslinjer.

Spørsmålet kan bli satt på spissen i arbeidsforhold, spesielt hvor arbeidsgiver har stilt IT-verktøy til disposisjon for arbeidstakeren i forbindelse med hans virke. Denne problemstillingen har ikke vært drøftet av rettspleien i dybden, og det er også lite teoretisk materiale rundt dette. Men det synes å være klart at dersom arbeidsgiver har instruks, retningslinjer eller avtale med arbeidstaker, kan arbeidsgiver gå inn på arbeidstakerens områder (selv om de er private). Dette med bakgrunn i at arbeidsgiver ikke vil være "uberettiget" (også med bakgrunn i at arbeidsgiver eier utstyret), og vil da følgelig gå fri fra straffelovens § 145, 2. ledd.

I forhold til forskriftsforlaget vil tolkningen av straffelovens § 145 være en tolkningsfaktor, men ikke gi noe særlige svar i forhold til arbeidsgivers innsynsrett. Dette fordi at personvernloven regulerer ett annet forhold, og det vil kunne være spørsmål om arbeidsgiver er "uberettiget" når arbeidsgiver eier og stiller utstyret til disposisjon. Hertil kommer det at arbeidsgiver har et selvstendig ansvar for å ivareta sikkerheten, og drive virksomheten på en forsvarlig måte.

8.5 Offentlighetsloven og tilsvarende lover

I forhold til det offentlige inneholder ulike lover krav til dokumentasjon og innsyn.

Offentlighetsloven § 2 sier *"Forvaltningens saksdokumenter er offentlige så langt det ikke er gjort unntak i lov eller i medhold av lov"*. Det medfører at saksdokumenter skal lagres, jf arkivloven § 6, *"Offentlige organ pliktar å ha arkiv, og desse skal vera ordna og innretta slik at dokumenta er tryggja som informasjonskjelder for samtid og ettertid."*

For private bedrifter eller virksomheter finnes det ikke noen tilsvarende arkivplikt. Imidlertid inneholder uliker lover som regnskapsloven, hvitvaskingsloven, og bokføringsloven med flere bestemmelser om dokumentasjonsplikt. Dette gjelder både private og offentlige organer. Det kan være i private organers interesse at de har arkiv, for eksempel i forbindelse med avtaler, reklamasjoner med mer.

Selv om forskriftsforslags relasjon til offentlighetsloven og lagring av saksinformasjon i forhold til dette reiser mange spørsmål, diskuteres ikke dette i oppgaven. Men den nevnes her likevel ettersom det kan være en tolkningsfaktor i forhold til arbeidsgiver innsynsrett.

Selv om det ligger litt på siden bør likevel U.S. Patriot Act⁵³ og Sarbanes Oxley Act⁵⁴ nevnes sett i forhold til et globaliserings-synspunkt. Disse regelverkene gir selskapene, og ikke minst den amerikanske stat, rett til innsyn, og pålegger selskaper evnen til å dokumentere elektroniske hendelsesforløp med meget korte tidsfrister. Det pågår et tilsvarende arbeid i EU for å harmonisere dette regelverket i forhold til USA. Uavhengig av dette bør det anmerkes at norske selskaper som samhandler med amerikanske selskap, eller som er notert på amerikanske børser, vil påvirkes av de forhold som U.S. Patriot Act og Sarbanes Oxley Act beskriver.

Tilsvarende problemstilling vil man få hvis morselskapet for eksempel er amerikansk, og har et avdelingskontor i Norge. Problemstillingen kommer til syne hvis hele den tekniske infrastrukturen (for eksempel e-postservere med mer) ligger i USA og reguleres av amerikanske lover eller morselskapets retningslinjer. I USA prioriteres "Corporate syn", hvor et selskaps interesser står langt sterkere enn i Norge, og som kanskje i ytterste konsekvens medfører at det går på tvers av hva den norske lovgivningen ønsker å verne.

Disse spørsmål har ikke vært til behandling i rettspleien og også vært lite behandlet av juridisk teori. Siste problemstillingen diskuteres imidlertid ytterligere under punktet "Rettslige betraktninger".

9. Rettslig betraktninger

Under rettslige betraktninger vil man se på hjemmelsgrunnlaget for forskriftsforlaget. Deretter vil man ta opp konkrete problemstillinger som er forbundet med forskriftsforlaget slik det fremstår.

9.1 Rettslige betraktninger vedrørende e-post generelt

E-post er i dag et utbredt og naturlig kommunikasjonsverktøy, som benyttes i en rekke arbeidssammenhenger. Vanligvis vil det være en del av arbeidsgivers eiendom, og normalt være installert som et arbeidsverktøy. Arbeidsgivers eiendomsrett til e-postsystemet gir i seg selv ikke rett til å lese e-post, men arbeidsgiver står som regel fritt gjennom styringsretten til å

⁵³ Se http://www.fincen.gov/pa_main.html

⁵⁴ Se <http://www.sarbanes-oxley-forum.com/> og <http://www.soxlaw.com/>

bestemme hvordan systemet skal brukes⁵⁵. Rettslig sett er det heller ikke noe i veien for at arbeidsgiver legger ned et totalforbud mot privat bruk⁵⁶.

Som tidligere nevnt, består e-post av tre komponenter; selve meldingen, e-postadressen (for eksempel per.person@virksomhet.no), og e-postkassen (@virksomhet.no, kan sammenliknes med ordinær postkasse), jf punktet ”Gjeldende rett vedrørende e-post”.

I forhold til selve meldingsdelen er det ikke bestridt at denne kan anses som en personopplysning, jf Rt 2002 side 1500.

Når det gjelder e-postadressen, for eksempel per.person@virksomhet.no, tjener den tre formål. Den er virksomhetens e-postkasse (@virksomhet.no), videre er den en intern e-postkasse innad i virksomheten, samt en identifikator for den interne e-postkassen.

Dvs at per.person@virksomhet.no tjener to formål, det ene er å være en intern e-postkasse, og det andre er å være identifikator.

Trekker man en analogi til den tradisjonelle brevhåndtering, vil brevet først mottas (vi ser bort i fra personlig levering) i hovedpostkassen til virksomheten. Brevet kan gå gjennom flere sikkerhetssjekker, for eksempel røntgen for se at brevet ikke inneholder annet enn papir, før det ankommer postmottaket. Deretter vil brevet gå til postmottaket som fordeler dette til de interne postkassene til aktuell mottaker i bedriften.

Tilsvarende vil det være for e-post. E-posten vil først mottas av virksomhetens hovedpostkasse (@virksomhet.no). Deretter vil det foretas en rekke sikkerhetssjekker, for eksempel i forhold til virus, spam og innhold, før den når den interne e-postkassen (per.person@virksomhet.no) til den aktuelle mottaker som er per.person@virksomhet.no.

At selve identifikatoren, her per.person@virksomhet.no, kan anses som en personopplysning er ikke bestridt, men spørsmålet blir som den andre funksjonen, dvs at det også er en intern e-postkasse, at selve e-postkassen kan anses som en personopplysning.

⁵⁵ Se også side 14 i høringsnotatet.

⁵⁶ Se også side 30 i høringsnotatet.

I forskriftsforslaget § 9-2 (1), innføres en definisjon på personlige e-postkasse. Denne er definert som ”*personlig e-postkasse: e-postkasse ved virksomheten som er knyttet til en bestemt persons navn eller etter avtale skal være personlig*”.

Det innebærer at en e-postkasse som per.person@virksomhet.no anses å være privat⁵⁷. Videre sies det i forskriftsforslaget § 9-3 (hovedreglen) at ”*Arbeidsgiver har ikke adgang til å gjennomføre, åpne eller lese e-post i en ansatts personlige e-postkasse*”.

Det forskriftsforslaget legger opp til, er å definere selve e-postkassen som en personopplysning, og dermed begrense arbeidsgivers innsynsrett. Spørsmålet blir om forskriftsforslaget har hjemmel til å definere denne funksjonen som en personopplysning. Ser man hen til den fysiske verden hvor det står navn på den interne postkassen, kan navnet anses som en personopplysning, men spørsmålet blir om den fysiske postkassen som sådan også blir å anse som en personopplysning.

I Ot. prp nummer 92⁵⁸, uttaler utvalget i punkt 4.1.3 at ”*Utvalget går inn for å la den nye personopplysningsloven omfatte all elektronisk behandling av personopplysninger og manuell behandling når personopplysningene skal inngå i et register, jf § 3 første ledd i utvalgets forslag*”.

Og i punkt 16, ”Merknader til de enkelte paragrafer”, til § 1, ”*Lovens formål*”, at ”*Formålsbestemmelsen er ny i forhold til personregisterloven og følger bl.a. opp Stortingets vedtak 21. april 1994 der det heter at: ”Stortinget ber Regjeringen legge fram forslag til endringer i lov om personregistre, slik at loven får en formålsparagraf som slår fast retten til vern mot utilbørlig inngripen i menneskers privatliv.*”

Videre i forhold § 2, ”Definisjoner”, ”*I tvilstilfeller kan formålsbestemmelsen få betydning for hvor langt uttrykket ”personopplysning” rekker - det kan tenkes tilfeller der ordlyden i nr 1 isolert sett trekker i retning av at en opplysning er ”personopplysning”, men hvor personvern hensyn ikke kan begrunne at opplysningen vernes*”.

⁵⁷ Se side 25 i høringsnotatet hvor høringsnotatet diskuterer forskjellen mellom private og ikke private e-postkasser.

⁵⁸ Ot. prp 92, (1998-99), Om lov om behandling av personopplysninger (personopplysningsloven), se <http://www.regjeringen.no/nb/dep/jd/dok/regpubl/otprp/19981999/Otprp-nr-92-1998-99-.html?id=160088>

Dette kan tyde på at det åpnes for å kunne foreta en innskrenkende tolkning av begrepet ”personopplysning” der hvor personvern hensyn ikke begrunner at opplysningene vernes.

Ser man også hen til formålet med e-postkassen, er denne stilt til disposisjon av arbeidsgiver i forbindelse med arbeidstakers virke. Videre kan arbeidsgiver i kraft av sin styringsrett, jf forskriftsforslaget § 9-8, gi instruksjon om hvordan utstyret skal benyttes.

Dernest påligger det at arbeidsgiver også har et selvstendig ansvar for å drive en virksomhet forsvarlig i forhold til annen lovgivning, som for eksempel regnskapslovgivning, hvitvaskingsloven med mer. Ved at e-post benyttes mye i forbindelse med virksomhetsrelatert kommunikasjon, vil arbeidsgiver ha en legitim interesse av å påse at virksomheten drives forsvarlig og effektivt. Det har for eksempel blitt hevdet at e-post har vært benyttet ved innsidehandel og hvitvasking⁵⁹, og i flere etterforskningsaker har påtalemyndigheten lagt frem bevis hvor bedriftens e-post vært benyttet til straffbare handlinger.

Oppsummerer man dette, er spørsmålet om selve e-postkassen er en ”behandling når personopplysningene skal inngå i et register”. Videre om innsyn i selve e-postkassen representerer en ”utilbørlig inngripen”, sett opp mot at det åpnes for en innskrenkende tolkning av begrepet ”personopplysning”.

Ved spørsmålet om selve e-postkassen er en ”behandling når personopplysningene skal inngå i et register”, kan dette kanskje besvares bekreftende hvis man ser helt objektivt på formålet med personopplysningsloven, som er å verne om personlig integritet og privatlivets fred. Med dette som utgangspunkt vil det ikke bestrides at også der opplysningene er lagret, dvs e-postkassen i seg selv, er å anse som personopplysning. Dette kommer noe indirekte frem i forskriftsforslagets § 9-1, 2. ledd⁶⁰.

Neste spørsmål er om dette representerer en ”utilbørlig inngripen”, som er bakgrunn for hele loven.

I Kunnskapsforlagets blå språk- og ordbokstjeneste er utilbørlig definert som ”som strider mot rett og rimelighet” og med synonymene: forkastelig, illojal, upassende, usømmelig, utilstedelig”.

⁵⁹ Se side 16 flg, i Lov og rett i cyberspace om hvordan Internett benyttes til slike formål.

⁶⁰ Se også side 25 i høringsnotatet.

Dette betyr at det må en sterk inngripen til. Sett opp mot at lovgiver åpner for en innskrenkende tolkning av begrepet, samt arbeidsgivers styringsrett (jf her forskriftsforlagets § 9-8 vedrørende instruks og punktet nedenfor ”Interne rutiner og instruks”), formålet hvorfor ansatt har fått e-post i virksomheten, samt at arbeidsgiver har et selvstendig ansvar både ovenfor 3. part (for eksempel kontraktsforpliktelser, reklamasjoner etc) og å drive virksomheten forsvarlig i forhold til annen lovgivning, er det sannsynligvis neppe ”utilbørlig inngripen” i forhold til ansatt vedrørende arbeidsgivers innsynsrett i selve e-postkassen. Også de betraktningene som er gjort ovenfor både i forhold til menneskerettigheter og personvern på arbeidsplassen, trekker i samme retning.

Med at så mange rettslikefaktorer trekker i samme retning, kan det vanskelig ses at forskriftsforlaget har hjemmel til å fastsette at selve e-postkassen i seg selv som en personopplysning. Og via dette avkjære arbeidsgivers rett direkte innsyn i selve e-postkassen som virksomheten stiller til disposisjon. At arbeidsgiver i utgangspunktet ikke har rett til å lese privat e-post i e-postkassen er ikke bestridt, men poenget er at arbeidsgiver har rett til innsyn i selve e-postkassen med bakgrunn av de betraktninger som er gjort ovenfor.

Under forutsetning av at hjemmelgrunnlaget er tilstrekkelig for å avskjære arbeidsgivers innsynsrett i e-postkassen til ansatte i virksomheten, dukker det opp flere problemstillinger i forhold til forskriftsforlagets § 9-3 (hovedregel), at *”Arbeidsgiver har ikke adgang til å gjennomføre, åpne eller lese e-post i en ansatts personlige e-postkasse”*. Disse gjennomgås kort nedenfor.

9.2 Jurisdiksjon

En problemstilling som vil dukke opp er i forhold til jurisdiksjon. For eksempel kan det tenkes at morselskapet i USA har et avdelingskontor i Norge. Med bredbånd og Internettets natur kan det tenkes at hele infrastrukturen (med bakgrunn i bl.a. sikkerhetsmessige årsaker, som for eksempel backup, It-systemets oppetider, økonomiske grunner, kontrolltiltak med mer), befinner seg i USA – dvs at selve e-postserveren befinner seg hos morselskapet. I USA gjør et ”Corporate” syn seg gjeldende i langt sterkere grad enn i Norge.

Selv om forskriftsforslagets § 9-1, 4. ledd, sier ”*Kapittelet gjelder tilsvarende der behandlingen skjer ved hjelp av databehandler*”, kan det bli vanskelig hvis databehandleren ligger i utlandet og må i tillegg oppfylle et annet lands lovgivning, typisk her morselskapet.

Det er ikke uvanlig i USA at de ansatte (og ansatte i datterselskaper i utlandet) samtykker ved tiltredelse at bedriften har full innsynsrett i deres e-post, dette også sett i sammenheng med U.S. Patriot Act og Sarbanes Oxley Act. Etter norske forhold kan også dette anses som tilstrekkelig, ettersom personopplysningsloven § 2, 1. ledd, nummer 6, legger samtykke til grunn for å kunne behandle personopplysninger.

Selv om det norske datterselskapet er et selvstendig rettssubjekt i forhold til norsk lovgivning, kan det likevel i en slik konstellasjon vanskelig ses hvordan forskriftsforslaget kan gi det vernet som det gir anvisning på. Dette både fordi samtykke gis (vilkårene i personopplysningsloven oppfylles), og at utstyret og tjenestene også reguleres av andre lands lovgivning, samt morselskapets retningslinjer.

8.3 Virksomhetsrelatert e-post blir ”privat” e-post

En annen problemstillingen er at all e-post, uavhengig om det er privat eller virksomhetsrelatert, vil bli ansett som å være ”privat” når det kommer i den ansattes e-postkasse. Dette fordi den ansattes e-postkasse i følge forskriftsforslaget anses som privat sfære, og som arbeidsgiver ikke automatisk har innsyn i.

Legger man til grunn de objektive krav og formål med personopplysningsloven, vil man sannsynligvis gå langt utenfor formålet til personopplysningsloven når man inkluderer også virksomhetsrelatert e-post til å være ”privat” e-post. I så fall brytes de lovfestede og ulovfestede arbeidsrettslige regelverk, spesielt i forhold til arbeidsgivers styringsrett, og da særlig i forhold til virksomhetsrelatert post generelt, og arbeidsgivers selvstendige ansvar til å drive virksomheten forsvarlig.

8.4 Mellomlagring av e-post i forbindelse med informasjonssikkerhet

En problemstilling som også vil kunne dukke opp, er når e-posten kommer inn i selve hovede-postkassen, dvs @virksomhet.no, før den distribueres til mottakeren. Skal det være slik at e-posten allerede på dette tidspunktet skal anses som ”privat”, eller er det først når e-posten faktisk har kommet frem til mottakerens e-postkasse.

Tar man utgangspunkt i at e-post anses som ”privat” allerede i det den kommer til virksomhetens e-postserver (@virksomhet.no), vil man kunne få en konflikt med personopplysningsloven § 13, og personopplysningsforskriften kapittel 2 vedrørende informasjonssikkerhet. Dette er begrunnet i at arbeidsgiver ikke vil ha innsynsrett, og kan heller ikke foreta mottiltak mot skadelig kode i det han ikke kan åpne e-posten.

Tar man motsatt standpunkt, at e-posten ikke anses som ”privat” før den faktisk kommer inn i selve e-postkassen til ansatt, vil arbeidsgiver kunne oppfylle sine krav i forhold til personopplysningsloven § 13, og personopplysningsforskriften kapittel 2 vedrørende informasjonssikkerhet. Dette kan også stemme med arkivforskriften §§ 3-1, og 3-2, jf også offentlighetsloven § 2. Utgangspunktet er at avsender sender e-post til virksomheten (@virksomhet.no). I motsetning til tradisjonelle brev, kan man ikke skrive navnet til mottager før virksomhetsnavnet i en e-post for å indikere at e-posten er privat. Tanken er likevel at ”post til organet skal åpnes av arkivtjenesten” så lenge den ikke er privat, jf arkivforskriften.

Det fremkommer ikke noe særlig informasjon i høringsnotatet om denne problemstillingen. På side 20 i høringsnotatet, under overskriften ”*Sørge for tilstrekkelig informasjonssikkerhet*”, er det nevnt av arbeidsgiver har ansvar for informasjonssikkerheten, for eksempel i forbindelse med virus, spam, phishing.

Det kan tyde på, med utgangspunkt i forskriftsforslaget, dets formål, samt kommentaren på side 20, at man har valgt en mellomløsning på hvor e-posten allerede er ”privat” når den innkommer hovede-postkassen, men at arbeidsgiver kan benytte verktøy for å luke ut virus, spam, phishing og andre elementer som utgjør en sikkerhetsrisiko. Denne tolkningen kan anses som riktig, ellers ville hele forskriftsforslaget kunne uthules ved at arbeidsgiver vil kunne ha fullt innsyn i hovede-postkassen.

Legges denne tolkning til grunn, vil det kunne oppstå tre nye problemstillinger; den ene er spam, den andre er innholdskontroll, og den tredje automatiserte administrative systemer.

Når det gjelder i forhold til spam, er det slik at virksomhetene har satt opp en rekke filtre for å luke ut slik e-post. Problemet er at e-posten som havner i slike filtre kan være reell. Derfor er det ikke uvanlig at for eksempel IT-personell går igjennom all e-post som er fanget opp av

spamfilteret for se om e-posten er reell eller spam. I mange tilfeller vil det være vanskelig å se om en e-post er spam bare ut fra emnefeltet, og man må da åpne selve e-posten for å ta stilling til dette.

Tilsvarende vil det være for sikkerhetssystemer som er installert i forbindelse med innholdskontroll⁶¹.

I forhold til disse to situasjonene hjelper det derfor ikke bare med automatiserte sikkerhetsinnretninger, man må faktisk behandle e-post manuelt i tillegg. I korthet vil det kunne bety at arbeidsgiver ved å sette opp strenge sikkerhetsrutiner i medhold av personopplysningsloven § 13, jf personopplysningsforskriften kapittel 2, uthuler mye av forskriftsforslaget ved at arbeidsgiver da vil kunne få innsyn i e-posten ved hjelp av slike innretninger.

Bruken av opplysninger som vil kunne komme til arbeidsgivers kunnskap gjennom sikkerhetsrutiner, behandles under punkt ”Interne rutiner og instruks”.

8.5 Interne rutiner og instruks

Forskriftsforslagets regelverk skiller mellom om arbeidsgiver har lagd en instruks om bruk av datasystemene eller ei.

I høringsnotatet sies det på side 14 at;

”Et sentralt formål med forskriftsforslaget er derfor å skape forutberegnelighet for både arbeidstaker og arbeidsgiver i forhold til når arbeidsgiver kan foreta innsyn i elektronisk utstyr stilt til arbeidstakers disposisjon.

Virksomhetene er forskjellige. Det må antas at arbeidsgiver selv er nærmest til å vite hvilke løsninger som er nødvendige og praktiske på den enkelte arbeidsplass. Departementet mener derfor at den enkelte virksomhet innenfor gitte rammer bør ha mulighet til å velge rutiner som er tilpasset arbeidsplassen. Det er en naturlig konsekvens av styringsretten og eierskapet til

⁶¹ Dette er systemer som inneholder filtre som sjekker at definert konfidensiell informasjon ikke slipper ut av bedriften eller inn. Både ved mottak og utsendelse av slik informasjon gis det varsel til systemadministrator som da går gjennom e-posten manuelt.

det elektroniske verktøyet at arbeidsgiver kan instruere de ansatte med hensyn til bruken av dette.

”Forskriften legger derfor til rette for at arbeidsgiver tenker gjennom hvordan arbeidstaker skal kunne bruke arbeidsgivers utstyr før konflikt oppstår og – etter drøfting med arbeidstaker – gir instruks for bruk av virksomhetens elektroniske utstyr”.

Og på side 30;

”Instruksen kan bl.a. bestemme at brukeren ikke har lov til å benytte virksomhetens elektroniske utstyr til private formål, at søk på bestemte ord på Internett er forbudt og at det ved hjelp av virksomhetens elektroniske utstyr ikke skal sendes privat e-post eller foretas annen privat kommunikasjon.”

Det eneste instruksen ikke kan fastsette, er i følge forskriftsforslaget § 9-8, 3. ledd, at *”Det er ikke anledning til å bestemme at all e-post eller annen elektronisk kommunikasjon som mottas med virksomhetens elektroniske utstyr skal anses som virksomhetsrelatert.”* Dette vil bli kommentert under punktet ”3. parts interesser”.

Det er et alminnelig prinsipp at arbeidsgiver kan instruere en arbeidstaker hvordan arbeidet skal utføres og hvordan utstyret skal benyttes. Dette kommer også til uttrykk forskriftsforslaget § 9-8.

Isolert sett, slik forskriftsforslaget legger opp til, vil virksomheter som har instruks kunne fravike forskriftsforslaget i langt større grad enn de som ikke har laget instruks. Dette må kunne antas å være riktig, ettersom formålet med forskriftsforslaget er å skape forutberegnelighet på rettstomt område. Dette kommer også til uttrykk på side 6 i høringsnotatet hvor det sies at *”Dersom instruksen er fulgt, vil interesseavveiningen som regel falle ut til fordel for arbeidsgiver”, og ”Motsatt vil interesseavveiningen som regel falle ut til fordel for den ansatte dersom instruksen ikke er fulgt ved innsynet.”.*

Men det som er interessant er å se forskriftsforslaget § 9-8, i sammenheng med § 9-5 1. ledd, c), sett i forhold til personopplysningsloven § 13, jf personopplysningsforskriften kapittel 2, og § 7-11.

I forhold til personopplysningsloven § 13, jf personopplysningsforskriften kapittel 2, er arbeidsgiver pliktig til å ivareta informasjonssikkerheten i datasystemene hvor det behandles personopplysninger. Dette gjøres med en rekke sikkerhetsmekanismer, som bl.a. spam- og innholdsfiltere med mer.

I kraft av arbeidsgivers styringsrett innrømmes arbeidsgiver, jf forskriftsforslaget § 9-8, stor frihet til å fastsette instruks og retningslinjer i vid forstand for hvordan utstyret skal benyttes. Ved å legge svært strenge føringer på hvordan utstyret skal brukes, vil sikkerhetsmekanismene slå ut og man vil kunne ligge tett opptil grensen for overvåking, jf betraktningene vedrørende overvåking under punktet ”Overvåking”.

Forskriftsforslaget § 9-5, 1. ledd c), gir vid adgang for arbeidsgiver til å få innsyn i ansattes e-postkasse hvis *”sending av e-posten medfører grovt brudd på de plikter som følger av arbeidsforholdet, arbeidsreglement eller annet skriftlig regelverk”*.

Poenget vil være at sikkerhetsfiltrene vil være så strengt satt opp at de vil kunne gi melding om mange sikkerhetsbrudd i forhold til de instruks og rutiner som er satt opp. Det vil gi adgang for arbeidsgiver til å ikke bare å få innsyn i e-posten, men også e-postkassen til ansatte.

Det kan argumenteres mot at dette vil kunne gå mot forskriftens formål. Men i den forbindelse er det viktig å legge til grunn arbeidsgivers styringsrett til å utforme retningslinjer og instruks, i tillegg anmerkes at i ovennevnte situasjon tenkes det at man ikke har krysset grensene til overvåking. Videre kan arbeidsgiver argumentere med at en streng sikkerhetsregime i virksomheten vil kunne bidra til å ivareta sikkerheten i datasystemene, og myndighetenes dokumentkrav for eksempel i forhold Sarbanes Oxley Act.

Ved å legge ovennevnte systematikk til grunn, vil forskriftsforslaget kunne uthules. Det anmerkes at forskriftsforslagets § 9-5, 1. ledd c), nevner ”grovt brudd”. Høringsnotatet gir ikke anvisning på hva dette er, og det er usikkert om man skal legge arbeidsmiljølovens §§ 15-13, 15-14, dvs de tilfeller som leder til suspensjon eller endelig avskjed, til grunn. Eller om det er arbeidsgivers subjektive oppfatning av hva som er grovt brudd i forhold til instruks og

retningslinjer. Det er både for- og motargumenter for begge løsningene, og hvor skalaene for grovt brudd bør ligge er dermed noe usikkert.

I personopplysningsforskriften § 7-11, 3. ledd settes det skranker for hva opplysningene kan benyttes til. Her slås det fast at personopplysninger som fremkommer som følge av administrering eller for å oppklare brudd på sikkerheten i datasystemet, ikke senere kan behandles for å overvåke eller kontrollere den enkelte.

Utgangspunktet blir imidlertid at man ved ovennevnte systematikk setter personopplysningsforskriften § 7-11 delvis ut av funksjon, ved at man oppnår innsyn ved hjelp av sikkerhetsinnretninger som skal ivareta sikkerheten (man må undersøke hva som førte til sikkerhetsbruddet i forhold til forskriftsforslagets § 9-5, 1. ledd c). Spørsmålet blir om det er personopplysningsforskriften § 7-11 som skal gis forrang foran forskriftsforslagets § 9-5, 1. ledd c. Hvis så, antas det at denne vil kunne miste en del av sin funksjon, og motsatt.

9.6 Virksomhetens og 3. parts juridiske interesser

Det er her tenkt på 3. part hvor arbeidsgiver har juridiske forpliktelser ved fravær, samt automatiserte administrative systemer.

Som tidligere nevnt skiller forskriftsforslagets regelverk mellom om arbeidsgiver har lagd en instruks om bruk av datasystemene eller ei.

Har arbeidsgiver lagd en instruks, kan man i henhold til forskriftsforslaget § 9-4, 2. ledd kan bokstav a (3-dagers regelen) og b (videresending av e-post ved fravær) i § 9-4 avvikes.

Har ikke arbeidsgiver instruks, må arbeidsgiver vente i 3 dager før arbeidsgiver kan få innsyn i e-postkassen til ansatte.

Forskriftsforslaget § 9-4, 1. ledd c) kan sannsynligvis ses på som en snever generell regel i forhold til fravær. Denne regulerer forhold der ”det er god grunn til å tro at det er innkommet virksomhetsrelatert e-post og at behandlingen av denne av hensyn til virksomhetens drift ikke kan vente.”. Sett i lys av hvordan dagens e-postkommunikasjon fungerer, der avsender sender en e-post uten (hvis det ikke haster) å følge dette noe særlig opp før etter noe tid, blir spørsmålet hvordan arbeidsgiver skal få varsel om ”at det er god grunn til å tro” at det har

kommet inn virksomhetsrelatert e-post som er viktig? Høringsnotatet gir noe godt svar på dette spørsmålet. Se for øvrig eksemplet nedenfor med å gjøre e-postkassen inaktiv, som har paralleller til denne problemstillingen.

Det er gitt anvisning på hvordan arbeidsgiver skal forholde seg ved uforutsett fravær⁶², jf Forskriftsforslaget § 9-4, 3. ledd; ”Ved uforutsett fravær skal arbeidsgiver begrense behovet for at e-postkassen må åpnes, for eksempel ved å gjøre e-postkassen inaktiv.”.

Å sette e-postkassen inaktiv vil teknisk sett bety og gjøre den utilgjengelig⁶³. Det innebærer at e-postmeldingen ikke kommer frem til mottakers e-postserver. Vedkommende som sender melding vil som regel ikke få beskjed om at e-postkassen er inaktiv før etter en stund. Denne tiden kan variere avhengig av e-postsystem og belastning på systemet.

En kan tenke seg situasjoner der en e-postkasse er inaktiv, og 3. part sender e-post for eksempel i forhold til anbud, reklamasjoner, aksept av tilbud, avtale, i forhold til offentlige rettigheter med tidsfrister med mer, på en ettermiddag før vedkommende reiser bort. Det betyr at 3. part i teorien ikke får beskjed om at e-postkassen er inaktiv før noen dager senere, og fristene kan da være oversteget.

Ettersom det er lett å forfalske en e-post⁶⁴, også tidspunktet for sending, kan avsender bli møtt med at vedkommende ikke har overholdt sine frister selv om vedkommende i realiteten har gjort det.

Å gjøre e-postkassen inaktiv, jf forskriftsforslaget § 9-4, 3. ledd, kan derfor være uheldig i forhold til virksomhetens, eller 3. parts juridiske interesser.

En annen problemstilling vil kunne være i forhold til de virksomheter som ikke har laget en instruks. Tenker vi oss et eksempel hvor det finnes en avtale mellom virksomhet A og B. Avtalen går ut på at hvis en innretning X går i stykker skal virksomhet B svare innen 24 timer på hva som skal gjøres for utbedre denne, ellers står virksomhet A fritt til å reparere denne

⁶² Fravær som ikke er planlagt, for eksempel sykdom med mer.

⁶³ Hvis bruker Asin e-postkasse settes inaktiv, betyr det i utgangspunktet at når B sender e-post til A, vil A sin e-postserver avvise meldingen på tilsvarende måte som om A ikke finnes. I korthet betyr det at meldingen ikke når frem til A sin e-postserver med bakgrunn i at A ikke finnes i e-postsystemet.

⁶⁴ Se side 12 i høringsnotatet.

hos andre og belaste B for kostnaden. Kommunikasjonen vedrørende dette skal i utgangspunktet foregå via e-post. Denne type avtaler er ikke uvanlig i større produksjonsbedrifter i dag.

En kan tenke seg et eksempel der kontaktperson i virksomhet B er på reise, og ikke har tilgang til sin e-post. Situasjonen inntreffer og virksomhet A sender e-post og fristen starter å løpe. Etter to dager meddeler virksomhet A at innretning er blitt reparert hos virksomhet X og faktura sendes til virksomhet B. I et slikt eksempel vil ikke virksomhet B kunne ivareta sine juridiske interesser.

Motargumentet til eksemplet ovenfor kan være at da burde virksomhet B ha laget rutiner for å håndtere ovennevnte situasjon. Poenget er at dette er kun en av flere problemstillinger forbundet med fravær. Slik forskriftsforslaget er lagt opp, vil det kunne være flere tilfeller hvor den ene parten ikke vil kunne være i stand til å ivareta sine juridiske interesser.

I denne sammenheng kan det også nevnes automatiserte administrative systemer, selv om problemet her vil være litt annerledes. For å effektivere og ivareta både virksomhetens og 3. parts interesser, benyttes automatiserte administrative systemer⁶⁵ mer og mer. Denne problemstillingen er heller ikke tatt opp i høringsnotatet.

En tenker seg her A og B i respektive virksomheter, og at disse også har et godt forretningsmessig forhold. A har kjøpt en del innretninger og varer fra B. I en del forretningsforhold er det heller ikke uvanlig at man også har sosial omgang på ”byen”. Videre kan en tenke seg at A i forbindelse med en reklamasjon (på det standardiserte skjema) også skriver et personlig innhold i e-posten om siste fuktige tur på byen med B sin sekretær med påfølgende nattlige aktiviteter. A legger også ved noen ”avslørende” bilder av B når de var på byen sammen sist, og spør om B fikk ”napp” med hun som er på bildet.

Når denne e-posten sendes, vil det automatiserte administrative systemet gjenkjenne reklamasjonsskjema og hele e-posten vil kunne spres til flere personer i bedrift B. Dermed vil

⁶⁵ Dette er systemer som fungerer på følgende måte. A kjøper for eksempel noe av B. B oversender A ordrebekreftelser, fakturagrunnlag, reklamasjonsskjema etc på et standardisert skjema. Kontaktpunktet for A er B i bedrift B. A finner noe feil ved varen og sender inn reklamasjonsskjema til B via e-post. E-postserveren til bedrift B gjenkjenner reklamasjonsskjema og sender i tillegg en kopi av e-posten til regnskapsavdelingen (i tilfellet av faktureringshensyn), og en til teknisk avdeling, og kanskje også til avdelingsleder til B slik at saken følges opp.

denne type systemer uthule mye av det forskriftsforslaget tar sikte på å regulere, nemlig personvernaspektet. Poenget er at denne type systemer er på full fart inn i virksomhetene for å kostnadsoptimalisere disse – det antas at forskriftsforslaget neppe er i stand til å stoppe utviklingen på dette tekniske området.

Det kan hende at A har en berettiget forventning om at det kun er B som leser e-posten som A sender. I juridisk teori⁶⁶ har det vært anført at A ligger utenfor arbeidsgiver Bs kontroll sfære, og A bør vite at når vedkommende sender e-post til virksomheten, så kan den være gjenstand for innsyn. Problemstillingen har imidlertid ikke vært diskutert i høringsnotatet og rettstilstanden er usikker.

9.7 Eierskap til datasystemet og lukkede datanett

I merknadene til forskriftsforslagets § 9-1 står det på side 24 i høringsnotatet at ”*Det er en forutsetning at arbeidsgiver eier utstyret. Arbeidsgiver kan ikke med bakgrunn i denne forskriften kreve innsyn i kommunikasjon utført med den ansattes eget utstyr, eller utstyr tilhørende tredjepersoner.*”. E-post innbefattes under ordet kommunikasjon.

Sett i forhold til dagens situasjon, hvor ikke bare e-post sammenblandes ved at den både er privat og virksomhetsrelatert, sammenblandes også teknisk utstyr som enten er privat, eller eid av arbeidsgiver.

Det finnes i dag mange konstellasjoner vedrørende teknisk utstyr. I visse forhold betaler arbeidsgiver bare en delsum, og resten betales av arbeidstaker fordi arbeidstakeren ønsker å kjøpe en mer ”high-tech” innretning. Eller arbeidstakeren kjøper privat en innretning som også brukes i jobbsammenheng. På hjemmekontorer vil det kunne finnes både privat og utstyr fra arbeidsgiver osv. Utgangspunktet er at det er mange konstellasjoner, og det er mye sammenblanding av privat, og utstyr eid av arbeidsgiver.

Forskriftsforslagets utgangspunkt er at arbeidsgiver ikke har innsyn hvis arbeidsgiver ikke eier utstyret. I korthet innebærer det at der arbeidstaker bruker privat utstyr til for eksempel å lese e-post, vil arbeidsgiver være avskåret helt fra innsyn i vedkommendes e-postkasse.

⁶⁶ Se for eksempel Line Coll, Arbeidsrett - 2006 - Nr 03, Blir retten til personlig integritet på arbeidsplassen krenket ved arbeidsgivers innsyn i virksomhetsrelatert e-post?

Spesielt vil det gjelde i de e-postsystemer hvor lagring ikke skjer sentralt, men desentralt på hver enkelt klient (dvs arbeidstakerens PC eller PDA).

Arbeidsgiver kan via sin styringsrett, jf forskriftsforslaget § 9-8, ved instruks nekte at privat utstyr benyttes. Dette utgangspunkt kan lede til allmennaksepterte forventninger, og at effektivitetsgraden i enkelte bransjer⁶⁷ går ned, ettersom "high-tech" utstyr kjøpt helt eller delvis av arbeidstaker også kan komme arbeidsgiver til nytte.

Denne problemstillingen er ikke drøftet i høringsnotatet, og sett ut fra hvor mye privat og utstyr eid av arbeidsgiver sammenblandes i dag, vil det kunne føre til usikker rettstilstand.

En annen problemstillingen er lukkede nett. Disse kan være graderte⁶⁸, hvor det ikke er lov til å sende privat informasjon. Man bruker også her e-post som en utstrakt kommunikasjon, forskjellen her er at det er en lukket brukergruppe som har tilgang, og det er kun denne gruppen som kan sende e-poster til hverandre.

Det er usikkert om forskriftsforslaget også tar sikte på å regulere dette. I forskriftsforslagets § 9-8, 3. ledd, står det at "Det er ikke anledning til å bestemme at all e-post eller annen elektronisk kommunikasjon som mottas med virksomhetens elektroniske utstyr skal anses som virksomhetsrelatert."

Utgangspunktet med lukkede nett, for eksempel i forbindelse med operasjoner eller hurtige tiltak, er at alle i den lukkede brukergruppen skal kunne lese e-post til alle (alle har tilgang til alles e-postkasser) for å gjøre operasjonen så effektiv som mulig. I graderte nett er det i tillegg krav om loggføring, og at arbeidsgiver har full tilgang til alle e-postkasser for eventuelt å avklare sikkerhetsbrudd i medhold av sikkerhetsloven med dens forskrifter.

Det er vanskelig å finne hvilken tolkning som skal legges til grunn ettersom forskriftsforslaget ikke tar opp denne problemstillingen. Denne problemstillingen blir mer aktuell ettersom flere virksomheter innfører lukkede nett for å ivareta den interne sikkerheten i forhold til for eksempel patenter, foretningshemmeligheter med mer.

⁶⁷ For eksempel i IT-bransjen, der det er vanlig og akseptert at arbeidstaker i tillegg til det arbeidsgiver stiller til disposisjon, kjøper mer "high-tech" utstyr som også benyttes i arbeidssammenheng.

⁶⁸ Jf sikkerhetsloven med dets forskrifter.

9.8 Elever og studenter

Forskriftsforslaget legger opp til at forskriften også skal gjelde for elever og studenter, og at disse får samme rettigheter som arbeidstager i forskriftsforslaget. Høringsnotatet på side 25 gir en begrunnelse for dette.

Skoleelever er en gruppe hvor størstedelen antas å være mindreårige, helt ned til 6 årsalderen. I forbindelse med det nye kunnskapsløftet er det et krav om at skoleelever skal lære å benytte IT-verktøy. De fleste skoler har implementert et verktøy som heter ”class-fronter”. Via denne sendes e-post, oversikt over skolearbeidet, kontakt med lærer med mer.

Videre har skolen et ansvar og plikt i forhold til oppdragelse, veiledning og å passe på elevene⁶⁹. Behovet og plikten vil være større jo yngre elevene er, spesielt i forhold til e-post og Internett-bruk. Elevers forventning og private sfære i forbindelse med bruk av datautstyr anses å være relativt liten, spesielt jo yngre barna er. Dette særlig sett i forhold til at skolen er også en oppdragelses- og veiledningsanstalt.

Utgangspunktet for denne problemstillingen er at det kan vanskelig ses hvordan en seks- eller tiåring, skal forvare sine plikter ut fra det komplekse regelverket som forskriftsforslaget legger opp til. Eller skal det være slik at ettersom barnet er mindreårig, at det skal representeres av sine foresatte eller andre.

I forhold til denne problemstillingen er det usikkert hva forskriften egentlig gjør forsøk på å regulere, ettersom det ikke kommer frem i høringsnotatet. Hvis det er slik at elever skal gis samme rettigheter som ansatte, vil spesielt grunnskolen vi avskåret fra innsyn. Det vil kunne innebære at grunnskolens ansvar og plikt i forhold til oppdragelse, veiledning og å passe på elevene kan bli vanskeliggjort.

I forhold til studenter kan situasjonen kanskje være motsatt. Dette begrunnet med at lærerstedet kanskje har mindre behov eller grunn til å følge med på studenters virke. I tillegg vil studenter kunne ha evnen til å forstå regelverket og ha behov for en privat sfære i likhet med ansatte. Her kan det tenkes situasjoner hvor studenten har forsket frem en unik innretning

⁶⁹ Jf det nye kunnskapsløftet i skolesektoren, se <http://www.regjeringen.no/nb/dep/kd/tema/andre/Kunnskapsloftet.html?id=1411>

og kommuniserer denne med en annen student – i slike tilfeller vil studenten ha berettiget krav mot innsyn i sine arbeider.

9.9 Arbeidsforholdet opphører

Det en her tenker seg er den situasjonen at arbeidstakeren dør. I forhold til forskriftsforslaget § 9-6 skal ” Når arbeidsforholdet opphører skal ansattes personlige e-postkasse i virksomheten avsluttes og innholdet slettes, hvis ikke annet er skriftlig avtalt eller går frem av instruks etter § 9-8.”.

Videre på side 29 i høringsnotatet at ”*De pårørende etter dødsfall har ikke uten videre krav på innsyn i den avdødes e-post mv. Det samme gjelder dødsboet. Dette må vurderes konkret etter §§ 8, 9 og 11. Hensynet til eventuelle tredjepersoner skal veie tungt.*”

Forskriftsforslaget legger opp til at hensynet til tredjepersoner skal veie tungt, og at ansattes personlige e-postkasse i virksomheten avsluttes og innholdet slettes. Det kan være situasjoner hvor e-postkommunikasjonen inneholder større immaterielle verdier. Eller privatrettslige kontrakter med mer. En automatisk sletteplikt slik forskriftsforslaget legger opp til, kan derfor være uheldig i forhold til disse rettighetene.

Et spørsmål er at viktige virksomhetsrelaterte opplysninger som er av bevaringsmessig verdi kan gå tapt ved en automatisk sletteplikt. I virksomheter som foretar kontraktsinngåelser, vil det ofte være nødvendig å kunne bevare all korrespondanse som vedrører kontraktsinngåelsen, i tilfelle det senere oppstår tvist knyttet til kontrakten. Å pålegge en automatisk sletteplikt i forhold til slike forhold kan også være uheldig.

9.10 Samtykke

I følge personopplysningsloven § 11 bokstav a), kan personopplysninger kun behandles når dette er tillatt etter personopplysningslovens §§ 8 og 9. Personopplysningsloven § 8 oppstiller flere vilkår for å kunne behandle personopplysninger. De kan behandles dersom den registrerte har gitt sitt samtykke, eller at det er fastsatt i lov, eller at behandlingen er nødvendig for de opplistede fastlagte behandlingsformål.

I forhold til denne problemstillingen som behandles, er samtykke og personopplysningsloven § 8 bokstav f) som behandlingsgrunnlag som er mest relevant. Personopplysningsloven § 8

bokstav f) gir anvisning på en interesseavveining. Personopplysninger kan behandles dersom det er nødvendig for at den behandlingsansvarlige skal kunne ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Også Datatilsynets praksis⁷⁰ viser at de behandlingsgrunnlag som oftest påberopes er henholdsvis samtykke og interesseavveining etter personopplysningslovens § 8 bokstav f. Interesseavveining etter personopplysningslovens § 8 bokstav f behandles ikke i oppgaven, med bakgrunn i oppgavens omfang.

Personopplysningsloven legger generelt stor vekt på samtykke, i samsvar med prinsippet om retten til selv å bestemme over opplysninger om seg selv. I følge juridisk teori og rettspraksis er det i utgangspunktet ingen formkrav til samtykket, men det må være uttrykkelig, frivillig og informert (dvs i form av en erklæring fra arbeidstakeren om at vedkommende godtar behandling av opplysninger om seg selv). Det er den behandlingsansvarlige (arbeidsgiver i dette tilfellet) som har bevisbyrden for at slikt samtykke er gitt.

I følge juridisk teori og rettspraksis er det antatt at det stilles strengere krav til samtykke hvis det er tale om et inngripende tiltak. Men det er antatt at et generelt samtykke vil være tilstrekkelig for de fleste ordinære tiltak. Det er sannsynligvis også adgang til å innhente forhåndssamtykke allerede i forbindelse med inngåelsen av arbeidsavtalen, hvis tiltaket ikke er for inngripende. I arbeidsforhold antas det at arbeidstaker gir sitt samtykke ved ansettelsen, og når vedkommende starter å bruke e-post i forbindelse med bruk av e-post.

I forhold til ulovfestede arbeidsrettslige prinsipper, kan det reises spørsmål om kollektivt samtykke er tilstrekkelig etter personopplysningsloven § 8, jf § 9. Personopplysningsloven og EUs personverndirektiv bygger på individuelt informert samtykke som hovedregel. Det er derfor antatt at den behandlingsansvarlige må innhente samtykke fra hver enkelt. Dette med bakgrunn i prinsippet om retten til selv å bestemme over opplysninger om seg selv. Det er derfor usikkert om en forening eller gruppe samlet sett kan gi samtykke på vegne av den enkelte i gruppen.

⁷⁰ Se side 5 i høringsnotatet.

Spørsmålstillingen er hvorfor samtykke ikke er nok i forhold til forskriftsforslaget § 9-8, 3. ledd. Høringsnotatet gir ikke noe godt svar på dette. Slik forskriftsforslaget er lagt opp virker det som om samtykke ikke er relevant også i forhold til resten av forskriftsforslaget. Samtykke er et sentralt begrep i forhold til personopplysningsloven, faktisk kan man ved samtykke la behandlingsansvarlige behandle sensitive opplysninger om seg selv, jf personopplysningsloven § 9. Spørsmålet blir da hvorfor sensitive opplysninger har mindre beskyttelsesverdi enn e-post?

Det virksom som nevnt ovenfor, at forskriftsforslaget avskjærer arbeidstaker samtykkeproblematikk. Dette må kunne sies å gå på tvers av personopplysningsloven vedrørende samtykke.

10. Sammendrag

Utgangspunktet for høringsnotatet er å sikre arbeidstaker vern mot arbeidsgivers innsyn, særlig med bakgrunn i argumentasjonen om at arbeidstaker har, sett ut fra dagens situasjon, rett til en privat sfære på arbeidsplassen. Videre at forskriftsforslaget, ikke bare i forhold til e-post, også kan inkludere nye teknologier som kan likne på e-post.

Det virker imidlertid mer som om forskriftsforslaget prøver å lage retningslinjer for en eksisterende teknologiplattform. Allerede nå er automatiserte administrative systemer, og ”ny” e-postvariant på full fart inn i næringslivet. Den ”nye” e-postvarianten inneholder en total sammensmelting av tale, video, utvidet meldingstjeneste (e-post slik vi kjenner det i dag blir bare en del av dette), posisjonering, betaling, lagring og søk i en og samme funksjon, med en identifikator for å identifisere eier av tjenesten.

Ved å prøve å lage retningslinjer for en teknologi vil man kunne komme ut feil, spesielt sett i forhold til den raske teknologiske utviklingen. En burde heller ha vurdert å skille mellom privat og virksomhetsrelatert e-post uten å ta utgangspunkt i selve teknologien.

Det er ubestridt at arbeidstaker har en privat sfære på arbeidsplassen. Hvis arbeidsgiver tillater at arbeidstaker kan bruke utstyr til privat gjøremål i arbeidstiden, kan arbeidsgiver gjøre dette på en enkel måte.

Noen virksomheter praktiserer to-delt system, hvor all kommunikasjon på e-postadressen per.person@virksomhet.no anses som virksomhetsrelatert, mens per.person.privat@virksomhet.no kan av arbeidstaker benyttes til private formål. Andre virksomheter tillater ikke at virksomhetens e-postadresse benyttes til private formål, men har lagt til rette for eksempel via en terminalserverløsning⁷¹ å nå sin egen private e-post.

Ved å heller ta utgangspunkt i privat og virksomhetsrelatert e-post og forsøke å regulere dette, istedenfor å ta utgangspunkt i en teknologi, antas det at forskriftsforslaget ville ha blitt mer fremtidsrettet og inkludere langt flere tilfeller som høringsnotatet ikke har vurdert. Med bakgrunn i dette antas det at forskriftsforslaget ville ha nådd sitt mål mer effektivt.

⁷¹ Dette er et system som ofte benyttes til å gi brukerne tilgang til Internett uavhengig av bedriftens system, dette spesielt i forhold til sikkerhetsperspektiv.

11. Litteraturliste

Torstein Eckhoff, Rettskildelære, 5. utgave ved Jan E. Helgesen

Personvern i informasjonssamfunnet - en innføring i vern av personopplysninger
Schartum, Dag Wiese og Bygrave, Lee A.

Elektronisk forvaltning i Norden- praksis, lovgivning og rettslige utfordringer
Schartum, Dag Wiese (red.)

Lov og rett i cyberspace, 2006, Inger Marie Sunde

Ot. prp 49 (2004 – 2005), Om lov om arbeidsmiljø, arbeidstid og stillingsvern mv.
(arbeidsmiljøloven)

Ot. prp 92, (1998-99), Om lov om behandling av personopplysninger
(personopplysningsloven)

NOU 2004:5, Arbeidslivslovutvalget
Underutvalgets rapport, "Kontroll og overvåking i arbeidslivet", avlevert 20. juni 2002 til
arbeidslivslovutvalget (NOU 2004:5).

NOU 1985:21, Datakriminalitet

NOU 2004:6, Mellom effektivitet og personvern - Politimetodeutvalget

SOU 2002:18, Personlig integritet i arbeidslivet

Transportøkonomisk institutt rapport 789/2005, "*Setter vår lit til Storebror ... og alle småbrødre med?* Befolkningens holdning til og kunnskap om personvern.

Transportøkonomisk institutt rapport 800/2005 *Behandling av personopplysninger i norske virksomheter*, En spørreundersøkelse om personvern og personopplysningsloven

Samtlige høringsuttalelser, se
<http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2006/Forslag-til-regler-om-arbeidsgivers-adgang-til-ansattes-e-post-mv/3.html?id=270945>

Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002

Kunnskapsløftet -
<http://www.regjeringen.no/nb/dep/kd/tema/andre/Kunnskapsloftet.html?id=1411>